http://dx.doi.org/10.21527/2317-5389.2017.9.201-236

As Transferências Transatlânticas de Dados Pessoais:
O Nível de Proteção Adequado Depois de *Schrems*

Alexandra Maria Rodrigues Araújo

Pesquisadora integrada no Centro de Estudos em Direito da União Europeia da Escola de Direito da Universidade do Minho (Braga, Portugal). Doutora em Direito pela Universidade de Navarra (Pamplona, Espanha). aaraujo.cedu@direito.uminho.pt.

Resumo

O princípio do nível de proteção adequado está no cerne da legislação de proteção de dados da União Europeia. Pressupõe que uma transferência para um país terceiro/organização internacional só seja permitida se estiver assegurado um nível adequado de proteção para os dados pessoais a transferir. Neste artigo analisa-se este princípio por meio de um estudo do conceito na legislação europeia sobre proteção de dados e, também, no recente acórdão *Schrems* do Tribunal de Justiça da União Europeia. Este acórdão tem uma importância crucial na interpretação deste princípio. Nele, o Tribunal esclarece, pela primeira vez, que este conceito exige ao país terceiro em questão assegurar um nível de proteção dos dados pessoais *substancialmente equivalente* ao conferido dentro da União Europeia. Desta forma, preserva-se uma certa margem de abertura para adaptar as apreciações de adequação às diferentes culturas e tradições jurídicas. Ao mesmo tempo reforça-se, a nível internacional, o direito à proteção de dados pessoais tal como está protegido na Carta dos Direitos Fundamentais da União Europeia.

Palavras-chave: Direito da União Europeia. Decisão de adequação. Dados de caráter pessoal. Direitos fundamentais. Princípios de porto seguro.

Transatlantic Data Transfers:
the adequate level of protection following the schrems rulling

Abstract

The principle of adequate level of protection is at the heart of the EU data protection legislation. It assumes that a transfer to a third country/international organization is only permissible if an adequate level of protection for personal data to be transferred is assured. This article analyses this principle through a study of the concept in European legislation on data protection and also in the recent Schrems judgment of the Court of Justice of the European Union. This judgment is of crucial importance in the interpretation of this principle. In it, the Court states that this concept requires that the third country in question ensures a level of protection substantially equivalent to that given in the European Union. Thus, it preserves a degree of openness to adapt the adequacy assessments to different cultures and legal traditions. At the same time, it strengthens internationally the right to data protection as it is ensured in the Charter of Fundamental Rights of the European Union.

Keywords: Personal data. Adequacy decision. Fundamental rights. EU law. Safe Harbour principles.

Sumário

1 CONSIDERAÇÕES INICIAIS

As Tecnologias da Informação e Comunicação (TICs) estão a trazer perspectivas surpreendentes e inovadoras para a economia e a vida social. Concomitantemente, o direito à proteção dos dados pessoais tem surgido como um contrapeso – cada vez mais necessário – no modo como estas tecnologias são utilizadas. Este direito é uma manifestação da dignidade de cada ser humano num mundo em que, poder assegurar um adequado controle da sua informação de caráter pessoal, adquire uma importância cada vez maior na construção da própria autonomia e identidade pessoal (FLORIDI, 2011). Vemos, contudo, que a garantia eficaz deste direito enfrenta constantemente novos desafios trazidos pela dinâmica evolutiva das TICs. Pois, tal como a tecnologia, a forma como os nossos dados de caráter pessoal são usados está em permanente evolução.

Um desafio à eficácia de qualquer legislação sobre proteção de dados são os seus fluxos transfronteiriços. As leis domésticas de proteção de dados perdem grande parte da sua eficácia com uma simples transferência desses dados para um país que não os proteja adequadamente. Hoje em dia, contudo, é impensável um mundo sem fluxos transfronteiriços de informação Como sublinham Fuster e Scherrer (2015), as atuais práticas de *big data,* muito dependentes da computação em nuvem, implicam que uma quantidade massiva de dados pessoais transpasse continuamente fronteiras geográficas e jurisdicionais. Além disso, há uma crescente necessidade de partilha transfronteiriça de informações por razões de segurança nacional. Partilha essa que, muitas vezes, tem sido feita à margem de uma estrutura legal adequada.

No Direito da União Europeia (UE) o princípio geral que se aplica a estes fluxos transfronteiriços de dados é o princípio do nível de proteção adequado. É um princípio que está no cerne da legislação de proteção de

dados da UE e pressupõe que uma transferência para um país terceiro/organização internacional só é permitida se estiver assegurado um nível adequado de proteção para os dados pessoais a transferir.

Este artigo tem por objetivo analisar a noção de nível de proteção adequado nas transferências, que têm por base jurídica uma decisão de adequação. O documento tem quatro partes. Na primeira é feita uma abordagem dos principais aspectos da legislação sobre proteção de dados da UE. A segunda parte do artigo apresenta o enquadramento jurídico geral das transferências internacionais de dados pessoais para países terceiros. A terceira parte é uma análise do conceito de nível de proteção adequado. Nesta parte a análise do acórdão *Schrems* é crucial. O artigo termina com breves reflexões sobre o conceito.

Por último, importa esclarecer que neste artigo utilizamos o conceito amplo de *dados pessoais* estabelecido no artigo artigo 2º al. a) da Diretiva 95/46/CE. São considerados dados de caráter pessoal "qualquer informação relativa a uma pessoa singular identificada ou identificável".[1]

2 QUADRO JURÍDICO DA PROTEÇÃO DE DADOS PESSOAIS NA UNIÃO EUROPEIA

Desde a entrada em vigor do Tratado de Lisboa (2009) que o artigo 16 do Tratado sobre o Funcionamento da União Europeia (TFUE) é o preceito-base da proteção de dados. O direito primário da UE o inclui no Título II do TFUE, que contém as disposições de aplicação geral. O número 1 do artigo reconhece o direito à proteção de dados de caráter pessoal; e no número 2 atribui-se à UE competência para legislar sobre a matéria em todas as áreas da sua incumbência.

[1] Para uma análise mais detalhada desta definição ver, por exemplo, Grupo de Trabalho de Proteção de Dados (2007, p. 6-23).

Quanto ao direito derivado, a Diretiva 95/46/CE do Parlamento Europeu e do Conselho de 24 de outubro de 1995 relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre-circulação desses dados (Diretiva de Proteção de Dados) é o principal instrumento jurídico da UE sobre proteção de dados. Os seus objetivos determinantes são: garantir a livre circulação de dados pessoais entre os Estados-Membros e proteger as liberdades e direitos fundamentais das pessoas singulares (naturais).

Além dos atuais 28 Estados-Membros da UE, a Diretiva de Proteção de Dados também se aplica aos Estados que fazem parte do Espaço Econômico Europeu (EEE) e que são a Islândia, o Liechtenstein e a Noruega (COMITÊ MISTO DO EEE, 1999). Este instrumento jurídico é complementado com outros. Por exemplo, a Decisão-Quadro 2008/977/JAI do Conselho, de 27 de novembro de 2008, relativa à proteção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal e que se aplica para a proteção de dados pessoais nestas matérias. Além disso, como a Diretiva de Proteção de Dados tem como destinatários os Estados, foi necessário adotar o Regulamento nº 45/2001 para proteger os dados de caráter pessoal do uso que as instituições, órgãos e organismos da UE façam deles. Por outro lado, também foi necessário detalhar algumas das disposições cobertas pela Diretiva de Proteção de Dados, tais como as relativas ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrônicas.

Sublinha-se que a Diretiva de Proteção de Dados é aplicável até 25 de maio de 2018. A partir dessa data é substituída pelo Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre-circulação desses dados e que revoga

a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).[2] Quer dizer, a partir de maio de 2018 o Regulamento Geral sobre a Proteção de Dados será diretamente aplicável em todos os Estados-Membros da UE.

Neste novo quadro jurídico da proteção de dados, os princípios e objetivos da Diretiva 95/46/CE são mantidos. O Regulamento, contudo, pretende adaptá-los aos desafios apresentados pela rápida evolução tecnológica e a globalização. O Regulamento Geral sobre a Proteção de Dados traz consigo mudanças significativas no âmbito das transferências de dados para países terceiros. De momento, destaca-se apenas a mudança do tipo de instrumento jurídico: de uma diretiva para um regulamento. A aplicabilidade direta do regulamento – tal como prevista no artigo 288 do TFUE – permitirá que um único instrumento jurídico vigore em toda a UE. Concordamos com autores, tais como Gilbert (2012, p. 817) e Gumzej (2012, p. 92), que defendem que, com esta mudança, muitas das complexidades e fragmentações jurídicas originadas pelas 28 leis nacionais que transpuseram a Diretiva 95/46/CE irão desaparecer.

2.1 O direito à proteção de dados pessoais como direito fundamental

A grande maioria dos instrumentos internacionais de proteção dos direitos humanos garante o direito à proteção de dados como uma extensão do direito à privacidade.[3] O direito primário da UE, contudo, dá

[2] A proposta de Regulamento Geral sobre a Proteção de Dados foi apresentada pela Comissão Europeia em janeiro de 2002 no âmbito do processo legislativo ordinário. O compromisso político sobre o conteúdo do regulamento foi alcançado informalmente em dezembro de 2015 pelas instituições intervenientes e, formalmente, em abril de 2016.

[3] No âmbito das Nações Unidas ver: Artigo 12 da Declaração Universal dos Direitos do Homem; Artigo 17 do Pacto Internacional sobre os Direitos Civis e Políticos; Comentário Geral n 16 sobre o respeito da privacidade, família, domicílio e correspondência, e proteção da honra e reputação – art. 17; Diretrizes para a Regulação de Ficheiros Informatizados de

um reconhecimento autônomo a este direito. A Carta dos Direitos Fundamentais da União Europeia (Carta) garante no artigo 7º o respeito pela vida privada e familiar e, no artigo 8º, o direito fundamental à proteção de dados pessoais.

Na verdade, desde que Warren e Brandeis (1890, p. 193-220) definiram o direito à privacidade como "the right to be left alone" as formas como a sociedade, o poder público ou outros indivíduos podem imiscuir-se nos assuntos pessoais de cada um evoluíram de forma drástica. Sabemos que, hoje em dia, a enorme quantidade de dados continuamente recolhidos e tratados proporciona um valioso instrumento informacional e comercial. Ao mesmo tempo, aumentaram exponencialmente os riscos de abusos no tratamento destes dados pessoais, assim como na sua utilização para fins ilícitos. Consequentemente, esta autonomia dada à proteção de dados pessoais é o reconhecimento do Direito à importância que o desenvolvimento tecnológico adquire na atual sociedade e é, portanto, uma tentativa de acompanhar este desenvolvimento. Este direito proporciona determinadas garantias às pessoas que vêm os seus dados pessoais serem tratados pelas Tecnologias da Informação. A proteção dos dados de caráter pessoal é, cada vez mais, um pressuposto fundamental em qualquer sociedade democrática, pois permite aos seus cidadãos desenvolverem livremente a sua personalidade e autonomia. Tal como acentua Ferretti (2014, p. 849),

Dados de Carácter Pessoal adotadas pela resolução 45/95 da Assembleia Geral das Nações Unidas em 14 de dezembro de 1990; Resolução 68/167 *Right to Privacy in the Digital Age* adotada pela Assembleia Geral das Nações Unidas em 18 de dezembro de 2013. No âmbito da Organização para a Cooperação e Desenvolvimento Econômico ver: *Guidelines governing the protection of privacy and transborder flows of personal data* (1980, revisão de 2013). Quanto aos instrumentos do Conselho da Europa destacam-se: o artigo 8 da Convenção Europeia dos Direitos do Homem; Convenção para a Proteção das Pessoas Relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal (Convenção 108) que entrou em vigor na ordem jurídica internacional a 1º de outubro de 1985 e posterior Protocolo Adicional (2004).

sem esta proteção rapidamente nos transformaremos em sociedades controladoras, de vigilância e fundamentadas em classificações das pessoas por perfis – atuais ou preditivos – potencialmente discriminatórios.

A jurisprudência do TJUE ainda não distingue com claridade a autonomia entre privacidade e proteção de dados. Não obstante, nós concordamos com os autores – tais como Hustinx (2015, p. 50) – que defendem que há diferenças a assinalar entre ambos os direitos. O direito à proteção de dados pessoais proporciona proteção jurídica às pessoas naturais contra o uso indevido das Tecnologias da Informação no tratamento das informações pessoais que lhes digam respeito. Pode ser qualquer tipo de informação. Quer dizer, esta proteção pode ser mais ampla que a proporcionada pela proteção da privacidade abrangendo informações que podem ou não incluir-se no âmbito do direito ao respeito à vida privada. Por outro lado, este direito pode ter um âmbito mais limitado que o da privacidade porque só se aplica ao tratamento de dados de caráter pessoal por meios total/parcialmente automatizados ou ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros ou a eles destinados.

O artigo 8º da Carta consagra o direito à proteção de dados pessoais e especifica no número 1 que estes dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. O artigo 8º número 2 garante o direito de todas as pessoas a aceder aos dados coligidos que lhes digam respeito e, se necessário, de obter a sua respectiva retificação. O número 3 do artigo estabelece que o cumprimento destas regras fica sujeito à fiscalização por parte de uma autoridade independente.

O direito à proteção de dados não é absoluto e, por isso, as restrições estabelecidas no artigo 52 número 1 da Carta podem ser aplicadas. Este direito pode ser restringido quando a restrição – na estrita observância do princípio da proporcionalidade – esteja prevista por lei; respeitar o conteúdo essencial do direito; for necessária e corresponder efetivamente

a um objetivo de interesse geral da UE ou, então, à necessidade de proteção dos direitos e liberdades de terceiros.[4] Tal como sublinha o Tribunal de Justiça da União Europeia (TJUE) no acórdão *Digital Rights Ireland*, no entanto, estas limitações devem ser sempre aplicadas de forma restrita (2014, par. 52).[5]

Outra das novidades introduzidas pelo Tratado de Lisboa encontra-se na atual redação do artigo 6º do Tratado da União Europeia (TUE), no qual se reconhece que a Carta tem o mesmo valor jurídico que os Tratados. A Carta, que durante anos apenas teve um inquestionável valor político, passou a ser juridicamente vinculativa para as instituições e Estados-Membros quando aplicam o Direito da UE (artigo 51 número 1). Desde então, este instrumento tornou-se um documento de referência obrigatória na hora de examinar a legalidade da legislação da UE.

[4] Para uma análise mais detalhada deste aspecto ver, por exemplo, Mangas Martín (2008, p. 832-837).

[5] O acórdão *Digital Rights Ireland* tem origem num pedido prejudicial de apreciação da validade da Diretiva 2006/24 relativa à conservação de dados à luz dos direitos fundamentais ao respeito pela vida privada e à proteção dos dados pessoais. O pedido visava a saber se a obrigação que a diretiva estipulava aos fornecedores de serviços de comunicações eletrônicas de conservar, durante um determinado período, dados relativos à vida privada de uma pessoa e às suas comunicações e de permitir o acesso a eles às autoridades nacionais competentes comportava uma ingerência injustificada nos referidos direitos fundamentais. O TJUE declarou que estas disposições da Diretiva 2006/24 constituíam uma ingerência particularmente grave no respeito pela vida privada e na proteção dos dados pessoais. Em seguida, em conformidade com o artigo 52 número 1 da Carta, o TJUE constatou que esta ingerência pode ser justificada, contudo o mesmo Tribunal entendeu que a diretiva era inválida por considerar que comportava uma ingerência nestes direitos fundamentais de grande amplitude e particular gravidade, sem que essa ingerência fosse enquadrada com precisão por disposições que permitissem garantir que se limitava efetivamente ao estritamente necessário.

3 BASE JURÍDICA DAS TRANSFERÊNCIAS DE DADOS PESSOAIS PARA FORA DO ESPAÇO ECONÔMICO EUROPEU

Os fluxos transfronteiriços de dados para fora do EEE estão regulados nos artigos 25 e 26 da Diretiva de Proteção de Dados e podem ocorrer por meio de diferentes bases jurídicas. A distinção mais importante é aquela que a legislação faz entre o livre fluxo de dados e o fluxo de dados restrito. Há livre fluxo de dados para países terceiros com um nível de proteção reconhecido como adequado mediante uma decisão de adequação; ou, ao abrigo das derrogações previstas no artigo 26. Nos outros casos, a transferência de dados para países terceiros pode realizar-se desde que sejam adotadas medidas especiais que assegurem a existência de garantias adequadas de proteção dos dados transferidos. Isto é, por meio de cláusulas contratuais, regras vinculativas para as empresas ou acordos internacionais especiais. Em particular, a UE tem celebrado acordos especiais para dois tipos de transferências de dados: para registos de identificação dos passageiros (PNR) e para dados de mensagens de pagamentos financeiros (TFTP: Programa de Deteção de Financiamento do Terrorismo).

3.1 A noção de transferência de dados pessoais

A noção de transferência de dados pessoais não está definida no Direito da UE.[6] Há, no entanto, vários elementos que ajudam a elucidá-la. Em primeiro lugar, a transferência tem de ser de *dados pessoais*. Em segundo lugar, importa considerar que o âmbito de aplicação do número 1 do artigo 25 da Diretiva 95/46/CE são as *transferências* de dados pessoais "objecto de tratamento ou que se destinem a ser objecto de tratamento

[6] Em âmbito internacional tampouco encontramos uma definição uniforme para *transferência de dados pessoais*. Neste sentido, ver Kuner (2013, p. 11).

após a sua transferência [...]". Para a interpretação deste artigo é necessário ter em conta o recente acórdão *Schrems,* no qual o TJUE esclarece que "a transferência de dados pessoais de um Estado-Membro para um país terceiro constitui, enquanto tal, um tratamento de dados pessoais." (2015, par. 45).

O conceito de transferência de dados pessoais também foi objeto da atenção do TJUE no acórdão *Boldil Lindqvist,* em que especifica que não há tal transferência

> […] quando uma pessoa que se encontra num Estado-Membro insere numa página Internet, armazenada num fornecedor de serviços de anfitrião que está estabelecido nesse mesmo Estado ou noutro Estado-Membro, dados de carácter pessoal, tornando-os deste modo acessíveis a qualquer pessoa que se ligue à Internet, incluindo pessoas que se encontram em países terceiros […] (2003, par. 71).[7]

Consequentemente, apenas as comunicações dirigidas a destinatários específicos podem ser abrangidas por esta noção (AGÊNCIA..., 2014, p. 131). Quer dizer, a informação necessita de estar deliberadamente disponível para destinatários no país terceiro. Desta forma, o conceito de transferência de dados pessoais exclui, também, as situações de mero trânsito dos dados pelo território de um Estado terceiro.

Apesar dos elementos referidos, discernir quando estamos perante uma transferência de dados pessoais pode tornar-se difícil e ainda depende de uma cuidadosa análise das circunstâncias do caso concreto. Como ponto de partida seguimos o entendimento da Autoridade Europeia para a Proteção de Dados (AEPD) quando destaca que a noção pode incluir

[7] . Este acórdão surgiu no contexto de um reenvio prejudicial colocado no âmbito de um processo penal pendente no *Göta hovrat* contra B. Lindqvist, acusada de ter violado a legislação sueca relativa à proteção dos dados de caráter pessoal ao publicar no seu *site* de Internet dados pessoais relativos a várias pessoas que trabalhavam com ela na paróquia de uma Igreja.

os seguintes elementos: *communication, disclosure or otherwise making available of personal data, conducted with the knowledge or intention of a sender subject […] that the recipient(s) will have access to it* (2014, p. 6-7).

3.2 As transferências internacionais de dados pessoais ao abrigo de uma decisão de adequação

O princípio do nível de proteção adequado é a regra geral que se aplica às transferências internacionais de dados pessoais ao abrigo de uma decisão de adequação. Segundo o artigo 25 número 1, este princípio implica que os fluxos de dados de caráter pessoal para países fora do EEE – chamados países terceiros – só sejam admissíveis se o país em questão garantir um nível adequado de proteção dos dados transferidos.

Ao abrigo da Diretiva 95/46/CE, a constatação do nível de proteção adequado pode ser realizada a diferentes níveis: a nível dos Estados-Membros e da Comissão Europeia. Os Estados-Membros utilizaram ao longo dos anos diferentes procedimentos administrativos para dar cumprimento a esta norma. Nomeadamente, por meio da imposição de uma obrigação direta aos responsáveis pelo tratamento dos dados; ou pelo desenvolvimento de um sistema de autorização prévia ou de controle posterior por parte das autoridades nacionais de proteção de dados (Comissão Europeia, 2003, p. 18-19). No novo Regulamento Geral sobre a Proteção de Dados, os Estados-Membros deixam de ter a possibilidade de fazer estas avaliações de adequação.

A Comissão Europeia também é competente para avaliar a adequação do nível de proteção de dados pessoais em países terceiros. A adoção de uma decisão de adequação pela Comissão Europeia pressupõe um processo que envolve uma proposta da Comissão; uma opinião do

Grupo de Trabalho do Artigo 29; a sua aprovação pelos representantes dos Estados-Membros e, por fim, a sua publicação no Jornal Oficial da União Europeia (Joue).

A decisão da Comissão é obrigatória em todos os Estados-Membros do EEE e garante a livre transferência de dados pessoais para o país terceiro em questão abrindo a esses países um acesso privilegiado ao mercado europeu. A qualquer momento, no entanto, o Parlamento Europeu e o Conselho, quando entendam que a Comissão excedeu os poderes de execução previstos na Diretiva de Proteção de Dados, podem solicitar que esta mantenha, altere ou retire uma decisão de adequação.

A Comissão tem feito avaliações de todo o sistema jurídico de um país, de parte desse sistema ou delimitado a sua avaliação a um só setor. Até os dias atuais, apenas um grupo restrito de países beneficiou de uma decisão de adequação: Andorra, Argentina, Canadá (legislação comercial), Suíça, Ilhas Faroé, Guernesey, Israel, Ilha de Man, Jersey, Nova Zelândia, Uruguai e aos *International Safe Harbour Principles* (princípios internacionais de porto seguro) do Departamento de Comércio dos EUA (para certas atividades do sector privado). Deste grupo, cabe destacar os dois países da América Latina com uma decisão de adequação. A Argentina beneficia de um acordo de partilha de dados desde 2003 (Comissão Europeia, 2003) e o Uruguai desde 2012 (Comissão Europeia, 2012). Além disso, o Uruguai foi o primeiro país não europeu a adotar a Convenção para a Protecção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal do Conselho da Europa.[8]

[8] A Convenção 108 entrou em vigor na ordem jurídica internacional a 1º de outubro de 2015 e tem como objetivo proteger os indivíduos contra os abusos que possam ser cometidos na recolha dos seus dados de caráter pessoal. Este instrumento internacional foi o primeiro juridicamente vinculativo no âmbito da proteção de dados. Todos os Estados-Membros da UE pertencem ao Conselho da Europa e ratificaram a Convenção 108, que tem um caráter aberto à adesão de Estados que não pertençam ao Conselho da Europa. Para uma análise mais detalhada da proteção de dados nos instrumentos do Conselho da Europa ver, por exemplo: RODRIGUES ARAÚJO, A.; OLIVEIRA, J. As transferências de dados pessoais

Recentemente a eficácia de algumas das decisões de adequação da Comissão Europeia têm sido fortemente questionadas em virtude do escândalo da vigilância eletrônica em larga escala a cidadãos da UE efetuada para fins de inteligência e segurança nacional. Em especial, foram seriamente questionadas as garantias de proteção de dados pessoais proporcionadas pelos princípios *Safe Harbour* (PARLAMENTO..., 2014). Uma vez que as empresas identificadas nas revelações dos meios de comunicação como estando envolvidas nesta vigilância massiva e indiscriminada a cidadãos europeus, são organizações que declararam a sua adesão a estes princípios. Estas revelações minaram seriamente a confiança e credibilidade dos princípios *Safe Harbour.* De fato, estes princípios foram declarados invalidados pelo TJUE em outubro de 2015. O acórdão será visto com mais detalhes ainda neste artigo.

4 O CONCEITO DE NÍVEL DE PROTEÇÃO ADEQUADO

A Diretiva Proteção de Dados não providencia uma definição do conceito de nível de proteção adequado. Não obstante, dá alguns critérios a seguir. O artigo 25 número 2 estabelece como critério principal que devem ser levadas em conta todas as circunstâncias que rodeiam a transferência ou o conjunto de transferências de dados. Em seguida oferece alguns critérios não exaustivos para a apreciação dessa adequação

> […] natureza dos dados, a finalidade e a duração do tratamento ou tratamentos projectados, os países de origem e de destino final , as regras de direito, gerais ou sectoriais, em vigor no país terceiro em causa, bem como as regras profissionais e as medidas de segurança que são respeitadas nesse país.

para países terceiros acompanhada de uma decisão de adequação no direito da União Europeia. *Direito e Novas Tecnologias I*. CONGRESSO NACIONAL DO COMPEDI/UFPB, 33.. Florianópolis: Compedi, 2014. p. 282-308.

Segundo o artigo 25 número 6, os critérios supramencionados devem ser aferidos pela Comissão Europeia por duas vias: mediante de uma análise da adequação oferecida pela legislação interna do país; ou por meio dos compromissos internacionais subscritos por esse país com vista à proteção do direito à vida privada e das liberdades e direitos fundamentais das pessoas.

4.1 A contribuição do Grupo de Trabalho do Artigo 29 para a noção de nível de proteção adequado

O Grupo de Proteção das Pessoas no que diz respeito ao tratamento de dados pessoais (Grupo de Trabalho do Artigo 29) é um grupo consultivo composto por representantes das autoridades de controle dos Estados-Membros, um representante da autoridade ou autoridades criadas para as instituições e organismos da UE e um representante da Comissão Europeia. Uma das atribuições do Grupo é emitir pareceres sobre o nível de proteção de países terceiros quando está em causa uma decisão de adequação. De fato, o parecer deste Grupo contribuiu significativamente para a construção interpretativa do conceito de nível de proteção adequado. Na sequência veremos os aspectos mais importantes da sua aportação.

Para o Grupo há dois elementos fundamentais na apreciação da adequação do nível de proteção oferecido por um país terceiro: a) a análise do conteúdo da legislação em vigor; e, b) a análise dos meios destinados a assegurar a sua efetiva aplicação.

Nas suas avaliações, o Grupo tem como referência o documento por ele adotado em 24 de julho de 1998 e intitulado "Transferência de dados pessoais para países terceiros: aplicação dos artigos 25 e 26 da Diretiva Comunitária relativa à proteção de dados". Neste documento de trabalho o Grupo, baseando-se na Diretiva de Proteção de Dados e noutros instrumentos internacionais de proteção dos direitos humanos, chegou a um conjunto de princípios substantivos nucleares da proteção de dados e de

quais os requisitos processuais cuja observância é indispensável para a existência de uma proteção adequada. Ainda assim, o Grupo considera que esta lista não pode ser interpretada de forma rígida para todas as transferências internacionais. O grau de risco que a transferência representa para a pessoa em causa é um elemento fundamental, que ajuda a determinar os requisitos específicos de proteção de dados no caso concreto.

Em geral, qualquer parecer de adequação do Grupo começa por identificar as normas sobre proteção dos dados pessoais do país terceiro: as leis consideradas como direito hierarquicamente superior e a legislação nacional que detalha a proteção de dados pessoais. Procede-se, em continuidade, a uma cuidadosa análise do seu grau de adequação. Analisa-se o âmbito material e territorial de aplicação da legislação e, também, a sua adequação com os princípios relativos ao conteúdo e aos mecanismos de aplicação efetiva do direito à proteção de dados pessoais considerados essenciais pelo Grupo.

Para o Grupo, os princípios básicos que devem estar necessariamente presentes no conteúdo de qualquer legislação nacional sobre a proteção de dados são: a) *Princípio da limitação da finalidade do tratamento*: os dados devem ser tratados para um fim específico e subsequentemente usados ou comunicados apenas na medida em que tal não seja incompatível com o fim da transferência inicial; b) *Princípio da proporcionalidade e da qualidade dos dados*: os dados devem ser exatos e, se necessário, atualizados. Devem, igualmente, ser adequados, relevantes e não excessivos em relação aos fins para os quais são transferidos ou posteriormente tratados; c) *Princípio da transparência*: o titular dos dados deve ser informado das finalidades do tratamento dos dados e da identidade do responsável pelo seu tratamento no país terceiro; d) *Princípio da segurança*: o responsável pelo tratamento dos dados deve tomar as medidas de segurança adequadas ao risco que o tratamento dos dados apresenta; e) *Direitos de acesso, de retificação e de oposição*: o titular dos dados tem o direito de obter uma cópia de todos os dados tratados a ele relativos, bem como o direito de retificação desses dados, caso se revelem inexatos. Em

determinadas circunstâncias a pessoa deve poder opor-se ao tratamento dos seus dados; f) *Restrições relativas a transferências subsequentes*: as transferências subsequentes de dados pessoais por parte do destinatário da transferência inicial só devem ser permitidas no caso de o segundo destinatário encontrar-se igualmente submetido a regras que garantem um nível de proteção adequado.[9]

O Grupo também estabelece quais os três objetivos principais de qualquer sistema jurídico de proteção de dados:

a) *Garantir um elevado nível de cumprimento das suas regras por parte dos responsáveis pelo tratamento de dados*. Para isso, os titulares dos dados devem ser conscientes dos seus direitos e de quais os meios que têm ao alcance para o seu exercício. A existência de sanções efetivas e dissuasivas é considerado um elemento importante que assegura a observância destas regras.

b) *Prestar apoio e assistência às pessoas cujos dados foram objeto de tratamento quando queiram exercer os seus direitos*. As pessoas devem poder exercer os seus direitos de forma rápida e efetiva, sem custos proibitivos. Para tal, deve existir um mecanismo institucional que permita a investigação independente das queixas;

c) *Fornecer meios de reparação adequados* à pessoa que sofreu danos devido ao não cumprimento das regras relativas à proteção de dados.

4.2 O acórdão *Schrems*

Este acórdão do TJUE é uma referência inquestionável para a interpretação do princípio do nível de proteção adequado (TJUE, 2015). Pela primeira vez este Tribunal centrou a sua atenção no conceito de nível

[9] O Grupo também estabeleceu princípios adicionais a aplicar quando estão em causa dados sensíveis, *marketing* direto e decisões individuais automatizadas.

de proteção adequado implícito no artigo 25 da Diretiva de Proteção de Dados. Por isso, nas próximas páginas faremos uma análise do caso destacando aqueles aspectos mais relacionados com este princípio.

4.2.1 Os fatos

Mr Schrems é um cidadão austríaco que reside na Áustria e é usuário da rede social Facebook desde 2008. Sabendo que os dados de caráter pessoal dos usuários do Facebook residentes no território da UE são transferidos para servidores em território dos Estados Unidos, Mr Schrems apresenta em 2013 uma queixa ao *Commissioner* (autoridade irlandesa que controla o respeito pela proteção de dados) pedindo a proibição da transferência dos seus dados pessoais para aquele país. Fundamentando-se nas revelações feitas por Edward Snowden, o queixoso alega que o direito e as práticas em vigor nos EUA não asseguram uma proteção suficiente dos dados pessoais conservados no seu território contra as atividades de vigilância aí exercidas pelas autoridades públicas, nomeadamente, pela Agência Nacional de Segurança (NSA) e pelo Federal Bureau of Investigation (FBI).

O *Commissioner* decide arquivar a queixa por falta de fundamento. Considera que não há provas de que a NSA tenha acessado os dados pessoais de Mr Schrems. Acrescenta, ainda, que as críticas suscitadas por Mr Schrems na sua queixa não podiam ser utilmente invocadas. O *Commissioner* argumenta que qualquer questão relativa ao caráter adequado da proteção dos dados pessoais nos EUA deve ser decidida em conformidade com a Decisão 2000/520, em que a Comissão Europeia constata que este país assegura um nível de proteção adequado aos dados pessoais transferidos, ao abrigo dos princípios internacionais de porto seguro.

Mr Schrems interpõe recurso da decisão do *Commissioner* para a *High Court* (Supremo Tribunal de Justiça). Este Tribunal entende que a vigilância eletrônica e a intercepção de dados pessoais transferidos da UE para os USA podem responder a finalidades necessárias e indispensáveis ao interesse público. Não obstante, a *High Court* constata, também, que após a transferência de dados pessoais para os Estados Unidos a NSA e outros órgãos federais, tais como o FBI, podem sujeitar os dados dos cidadãos europeus à vigilância e a intercepções massivas e indiscriminadas, sem que estes cidadãos disponham de nenhum direito efetivo de serem ouvidos.

A *High Court* lembra que a Constituição irlandesa exige que qualquer ingerência nos direitos a respeito da vida privada e à inviolabilidade do domícilio seja proporcionada e respeite os requisitos previstos pela lei. Por isso, este Tribunal entende que o acesso massivo e indiscriminado a dados pessoais é contrário ao princípio da proporcionalidade e aos valores fundamentais protegidos pela Constituição da Irlanda. Segundo este entendimento, para que as intercepções das comunicações eletrônicas sejam consideradas conformes com a Constituição irlandesa devem estar sujeitas ao cumprimento de uma série de requisitos cumulativos, tais como: apresentar provas de que as intercepções têm caráter seletivo; 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 existem garantias adequadas e verificáveis.

A *High Court,* todavia, considera que a legalidade da Decisão 2000/52 deve ser, também, questionada à luz do direito da UE. Especialmente, à luz dos requisitos dos artigos 7º, 8º e 51 da Carta. A *High Court* observa que M. Schrems faz, igualmente, um questionamento implícito da legalidade dos *Safe Harbour Principles* estabelecidos pela Decisão 2000/520. Assim sendo, coloca-se a questão de saber se – nos termos do artigo 25 número 6 da Diretiva de Proteção de Dados – o *Commissioner*

está vinculado à decisão de adequação da Comissão ou se o artigo 8º da Carta autoriza o *Commissioner* a questioná-la e a se afastar dessa constatação de adequação.

Foi nestas condições que a *High Court* decidiu suspender a instância e submeter ao TJUE as seguintes questões prejudiciais:

> 1) Tendo em conta os artigos 7.º, 8.º e 47.º da Carta […] e sem prejuízo das disposições do artigo 25.º, n.º 6, da Diretiva 95/46, o [Commissioner] encarregad[o] de aplicar a legislação sobre a proteção de dados pessoais no âmbito da análise de uma queixa segundo a qual o direito e as práticas de um país terceiro (neste caso, os Estados Unidos da América) para o qual são enviados dados pessoais não oferecem proteção adequada, está vinculado em termos absolutos pela constatação em sentido contrário da União, contida na Decisão 2000/520?
>
> 2) Em alternativa, pode e/ou deve proceder à sua própria investigação sobre a matéria, à luz dos últimos desenvolvimentos de facto ocorridos desde a primeira publicação da decisão da Comissão?

4.2.2 O Acórdão

Depois de apresentadas as Conclusões do Advogado Geral (AG) Y. Bot, o TJUE pronunciou-se sobre as questões prejudiciais submetidas em 6 de outubro de 2015.[10]O acórdão centrou-se na análise de três temas: a) quais os poderes das autoridades nacionais de controle perante uma decisão de adequação da Comissão Europeia; b) o conceito de nível de proteção adequado; c) a validade da Decisão 2000/520. Nas próximas linhas salienta-se o mais relevante de cada um destes aspectos.

[10] Composição do Tribunal: V. Skouris, presidente, K. Lenaerts, vicepresidente, A. Tizzano, R. Silva de Lapuerta, T. von Danwitz (relator), S. Rodin, K. Jürimäe, presidentes de secção, A. Rosas, E. Juhász, A. Borg Barthet, J. Malenovský, D. □váby, M. Berger, F. Biltgen e C. Lycourgos, juízes.

a) *Os poderes das autoridades nacionais de controle perante as transferências de dados pessoais realizadas ao abrigo de uma decisão europeia de adequação*

O Tribunal esclarece que o artigo 28 da Diretiva Proteção de Dados pressupõe, sempre, uma obrigação de verificar se uma transferência de dados pessoais do Estado-Membro dessa autoridade para um país terceiro respeita os requisitos estabelecidos pela Diretiva. O Tribunal esclarece que essa competência das autoridades nacionais inclui, igualmente, o poder para fiscalizar as transferências de dados pessoais para países terceiros que tenham sido objeto de uma decisão de adequação da Comissão. O Tribunal, entretanto, deixa claro que só o TJUE pode declarar a invalidade de uma decisão da Comissão adotada nos termos do artigo 25 número 6. A exclusividade desta competência tem por objetivo garantir a segurança jurídica e preservar a aplicação uniforme do direito da União (par. 38-39).

b) *O conceito de nível de proteção adequado*

O Tribunal lembra que a Diretiva de Proteção de Dados deve ser interpretada de forma a assegurar uma proteção completa e efetiva dos direitos e liberdades garantidos na Carta e um nível elevado de proteção das liberdades e direitos fundamentais das pessoas (par. 38-39).[11] Nesse sentido, a redação do artigo 25 número 6 implica que "a adequação da proteção assegurada pelo país terceiro é apreciada 'com vista à proteção do direito à vida privada e das liberdades e direitos fundamentais das pessoas'". Seguindo a opinião do AG Bot, o Tribunal enfatiza que o artigo 8º número 1 da Carta pressupõe a obrigação de dar continuidade a um nível elevado de proteção dos dados pessoais quando esses dados sejam transferidos para um país terceiro (par. 71-72).

[11] Ver também o acórdão *Google Spain and Google* (TJUE, 2014, par. 68).

O Tribunal, no entanto, esclarece um aspecto importante: assegurar um nível de proteção adequado não significa necessariamente "que um país terceiro assegure um nível de proteção idêntico ao garantido na ordem jurídica da União". Esta expressão

> […] deve ser entendida no sentido de que exige que esse país terceiro assegure efetivamente […] um nível de proteção das liberdades e direitos fundamentais substancialmente equivalente ao conferido dentro da União nos termos da Diretiva 95/46, lida à luz da Carta (par. 73).

Para o Tribunal, o nível de proteção essencialmente equivalente ao garantido dentro da UE deve ser apreciado na prática, contudo os meios a que esse país recorre para assegurar tal nível de proteção podem ser diferentes dos praticados dentro da UE (par. 74).

O Tribunal sublinha, igualmente, que a Comissão, na sua apreciação da adequação, deve apreciar o conteúdo das regras aplicáveis nesse país que resultem da sua legislação interna e dos seus compromissos internacionais. E, também, deve apreciar a prática destinada a assegurar o respeito a tais regras. Nesse sentido, deve considerar todas as circunstâncias relativas a uma transferência de dados pessoais para esse país terceiro (par. 75). Por último, o Tribunal lembra que a Comissão tem a obrigação de verificar periodicamente se a constatação relativa ao nível de proteção adequado assegurado pelo país terceiro continua a se justificar, quer de fato quer de direito (par. 76).

c) A validade da Decisão 2000/520

Depois de analisar o conteúdo da Decisão 2000/520, o Tribunal entende que o documento não apresenta constatações suficientes que assegurem um nível de proteção adequado. Sublinha, ainda, que a aplicabilidade dos princípios *Safe Harbour* apresenta uma derrogação de caráter geral segundo a qual estes princípios podem ser limitados por

> […] requisitos de segurança nacional, interesse público ou [cumprimento da lei], bem como por legislação, regulamento governamental ou jurisprudência que criam obrigações contraditórias ou autorizações explícitas, desde que, no exercício de tal autorização, uma organização possa demonstrar que o incumprimento dos princípios se limita ao necessário para respeitar os legítimos interesses superiores [prosseguidos] por essa autorização.

Quer dizer, a Decisão consagra o primado destes requisitos sobre os princípios *Safe Harbour*, sendo as organizações americanas autocertificadas obrigadas a afastar, sem qualquer limitação, esses princípios quando entrem em conflito com aqueles requisitos. Em consequência, o Tribunal entende que a Decisão 2000/520 não oferece aos cidadãos europeus uma proteção jurídica eficaz para ingerências desta natureza (par. 87-89).

Seguindo este entendimento, o Tribunal lembra que a jurisprudência constante do TJUE demanda que uma ingerência nos direitos fundamentais, garantidos pelos artigos 7º e 8º da Carta, deve

> estabelecer regras claras e precisas que regulem o âmbito e a aplicação de uma medida e imponham exigências mínimas, de modo a que as pessoas cujos dados pessoais estejam em causa disponham de garantias suficientes que permitam proteger eficazmente os seus dados contra os riscos de abuso e contra qualquer acesso e qualquer utilização ilícita desses dados (par. 91-92).

Além disso, a proteção do direito fundamental ao respeito da vida privada exige que as derrogações à proteção dos dados pessoais e as suas limitações operem na estrita medida do necessário. Desse modo, o Tribunal conclui que uma regulamentação, que permite às autoridades públicas acessar de modo generalizado ao conteúdo das comunicações eletrônicas dos cidadãos europeus, deve ser considerada lesiva do conteúdo essencial do direito fundamental ao respeito da vida privada, tal como garantido pelo artigo 7º da Carta (par. 93-94). Conclui, igualmente, que uma regulamentação que não preveja nenhuma possibilidade para o particular de recorrer a

vias de direito para ter acesso aos dados pessoais que lhe dizem respeito, ou para obter a retificação ou a supressão de tais dados, não respeita o conteúdo essencial do direito fundamental a uma proteção jurisdicional efetiva, tal como consagrado no artigo 47 da Carta (par. 95).

Na sequência o Tribunal analisa o artigo 3º da Decisão 2000/520 e constata que este priva as autoridades nacionais do controle de poder examinar, com total independência, qualquer pedido relativo à proteção dos direitos e liberdades de uma pessoa no que diz respeito ao tratamento dos seus dados pessoais. Por isso, o Tribunal conclui que a Comissão ultrapassou a competência que lhe foi atribuída pelo artigos 25 número 6, e 28 e, por isso, este artigo 3º é igualmente inválido.

À luz dos mencionados argumentos, o Tribunal entende que a Decisão 2000/520 não assegura um nível de proteção adequado e viola os requisitos estabelecidos no artigo 25 número 6 da Diretiva 95/48/CE. A Decisão 2000/520 é, por esta razão, inválida (par. 97-106).

4.2.3 O Princípio do Nível de Proteção Adequado depois de Schrems

O acórdão *Schrems* inviabilizou as transferências de dados UE-USA por meio da Decisão 2000/520. Em consequência, as transferências transatlânticas de dados pessoais para os USA precisam fundamentar-se nos instrumentos legais alternativos: nas cláusulas contratuais, nas regras vinculativas das empresas ou nos termos das derrogações específicas previstas no artigo 26 da Diretiva (COMISSÃO..., 2015b, p. 5-13). Não obstante, a importância das transferências transatlânticas de dados impulsionou a Comissão a iniciar negociações com vista à adoção de uma nova base

jurídica que facilite os fluxos de dados pessoais para fins comerciais.[12] O resultado foi um acordo político do Colégio dos Comissários com vista à adoção de uma nova decisão de adequação: o *EU-US Privacy Shield*.[13]

Em relação às restantes decisões de adequação adotadas pela Comissão, o âmbito do presente acórdão é apenas limitado à Decisão 2000/520 e, por isso, não as afeta. O Regulamento Geral sobre a Proteção de Dados também mantém em vigor as decisões de adequação já existentes o que não impede que possam ser alteradas, substituídas ou renovadas por uma nova decisão da Comissão.

a) *O Princípio do Nível de Proteção Adequado no Regulamento Geral sobre a Proteção de Dados*

Durante as discussões que precederam a adoção do novo Regulamento Geral sobre a Proteção de Dados, a reforma do quadro jurídico para as transferências individuais foi um dos pontos considerados mais necessários e importantes. É entendimento generalizado que, para a maioria dos cidadãos europeus, a atual Diretiva não conseguiu evitar nem uma fragmentação na execução destas transferências nem um nível alto de insegurança sobre os seus dados pessoais (COMISSÃO..., 2015a). Apesar de todos os esforços da UE para promover um elevado nível de proteção dos dados pessoais nas transferências internacionais, a realidade tem demonstrado que, na prática, a eficácia desta proteção tem ficado muito aquém das expectativas (KUNER, 2016).

[12] As relações econômicas entre os EUA e a UE são as mais significativas do mundo. Em 2014, o comércio total EUA-UE moveu 1,09 bilhão de dólares. Os fluxos transfronteiriços de dados entre os EUA e a Europa são os mais elevados do mundo. Comparando com outros blocos regionais constata-se que são 50% superiores aos fluxos de dados entre os EUA e a Ásia e quase o dobro dos fluxos de dados entre os EUA e a América Latina (PARLAMENTO..., 2016).

[13] A versão preliminar do documento encontra-se disponível em: <http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm>.

Quanto ao conceito de nível de proteção adequado, na falta de uma maior definição, foi sendo aplicado de uma forma funcional e casuística (AUTORIDADE..., 2014, p.10). Esta falta de clareza e detalhes foram fatores frequentemente apontados como causadores de dificuldades na interpretação do princípio, com a consequente fragmentação e insegurança jurídica que acarreta (ZINSER, 2004, p. 172; SCHWARTZ, 1994-1995, p. 473). A falta de uniformidade na interpretação do princípio foi reconhecida no âmbito da UE, por várias das suas instituições e organismos (AUTORIDADE..., 2011, p. 14; PARLAMENTO..., 2011, p. 4; COMISSÃO..., 2003, p. 18-20).

Durante anos, a noção de nível de proteção *adequado* foi questionada em relação à expressão nível de proteção *equivalente* (SCHWARTZ, 1994-1995, p. 472; HOEREN, 1993-1994, p. 140). Para algumas interpretações, o uso desta expressão parecia sugerir que não se exigia ao país terceiro em questão um nível de proteção dos dados pessoais equivalente ao da legislação europeia. A expressão foi entendida como pressupondo um nível de proteção inferior. Esta interpretação apoiava-se na comparação entre o considerando 8º da Diretiva de Proteção de Dados e o artigo 25 número 1. O considerando 8º requer um nível de proteção dos direitos e liberdades das pessoas no que diz respeito ao tratamento destes dados que seja *equivalente* entre todos os Estados-Membros. Pelo contrário, o artigo 25 número 1 utiliza a expressão *adequado*. Como sabemos, o acórdão *Schrems* esclareceu esta discussão.

Por todas estas razões, a reforma do quadro jurídico da UE sobre proteção de dados teve como um dos seus objetivos reforçar os procedimentos em vigor para as transferências internacionais de dados de modo a definir com mais rigor e clareza a avaliação do nível de proteção de dados

do país terceiro. No Regulamento Geral sobre Proteção de Dados os artigos referentes às transferências de dados pessoais para países terceiros ou organizações internacionais situam-se no Capítulo V (artigos 44 a 50).[14]

O artigo 44 do Regulamento intitula-se *Princípio Geral das Transferências.* Este artigo é uma das novidades do novo quadro-jurídico e, lido em conjunto com o artigo 3º, estabelece como premissa geral que sempre que bens e serviços sejam propostos a pessoas singulares residentes na UE, ou sempre que o seu comportamento seja controlado (desde que esse comportamento tenha lugar no território da UE), as regras a aplicar são as da UE. Também especifica que este princípio deve ser aplicado quer às transferências originais, quer às ulteriores.

Outra premissa identificada no mesmo artigo estabelece que uma transferência de dados para país terceiro só se pode realizar quando não comprometa o nível de proteção das pessoas singulares garantido pelo Regulamento Geral sobre a Proteção de Dados. Quer dizer, quando os dados dessas pessoas são transferidos para um país terceiro/organização internacional, deve ser mantido o nível de prote**ção** de que gozam pela legislação da UE. Este princípio está em consonância com o estipulado no acórdão *Schrems.*

Em consequência, o princípio do nível de proteção adequado – reafirmado no artigo 45 número 1 do Regulamento Geral – deve ser interpretado à luz deste novo preceito-chave. Um nível de proteção adequado é aquele que preserva o mesmo nível de proteção que que os dados pessoais gozam na UE. Além disso, o considerando 104 do Regulamento acolhe a interpretação dada pelo TJUE em *Schrems* e especifica que o princípio do

[14] Nas anteriores versões da proposta de Regulamento, o Capítulo V englobava os artigos 40-45.

nível de proteção adequado é respeitado quando o país terceiro dá "[…] garantias para assegurar um nível adequado de proteção essencialmente equivalente ao assegurado na União […]".

Em relação às decisões de adequação adotadas pela Comissão Europeia, o artigo 45 número 2 do novo Regulamento esclarece nas alíneas a), b) e c) quais os critérios a considerar na avaliação do nível de adequação. São eles: o primado do Estado de direito; o respeito pelos direitos humanos e liberdades fundamentais; a legislação relevante em vigor (geral e setorial); a aplicação dessa legislação e das regras de proteção de dados; as regras profissionais e as medidas de segurança que são cumpridas nesse país, a jurisprudência, os direitos dos titulares dos dados efetivos e oponíveis e as vias de recurso administrativo e judicial para os titulares de dados cujas informações pessoais sejam objeto de transferência; a existência e o efetivo funcionamento de pelo menos uma autoridade de controle independentes no país terceiro; os compromissos internacionais assumidos pelo país terceiro ou outras obrigações decorrentes de convenções ou instrumentos juridicamente vinculativos, bem como da participação em sistemas multilaterais ou regionais (em especial em relação à proteção de dados pessoais).

No novo quadro jurídico deixam, portanto, de fazer parte dos critérios de avaliação o conjunto de circunstâncias que rodeiam as transferências de dados. Além disso, da leitura do Capítulo V depreende-se que a decisão de adequação é centralizada na Comissão Europeia. Quer dizer, é negada a possibilidade de fazer esta avaliação de adequação no âmbito dos Estados-Membros.

O número 3 do mesmo artigo 45 explicita que a Comissão – depois de uma cuidadosa avaliação – pode decidir, por meio de um ato de execução, que um país terceiro, um território ou um setor de tratamento nesse país terceiro, ou uma organização internacional asseguram um nível de proteção adequado.

Outra novidade muito desejada é a formalização no Regulamento dos procedimentos de controle posteriores por intermédio de avaliações – quer periódicas, quer contínuas – da eficácia das decisões de adequação em vigor. Segundo o Artigo 45 número 3, no próprio ato de execução que adota uma decisão de adequação, a Comissão Europeia deve prever um procedimento de avaliação periódica, no mínimo de quatro em quatro anos, que deverá levar em conta todos os desenvolvimentos pertinentes no país terceiro/organização internacional. Além desta avaliação periódica, a Comissão Europeia tem a obrigação de controlar de forma continuada os desenvolvimentos nos países terceiros/organizações internacionais que possam afetar o funcionamento das decisões de adequação adotadas (número 4). Nos casos em que a Comissão Europeia constata que um país deixou de assegurar um nível de proteção adequado deve, na medida do necessário, revogar, alterar ou suspender a decisão de adequação. A Comissão deve, igualmente, iniciar consultas com vista a remediar a situação de inadequação. Por último, o artigo também compromete a Comissão com a publicação no Jornal Oficial da União Europeia (Joue) de uma lista dos países terceiros, territórios e setores de tratamento num país terceiro e de organizações internacionais relativamente aos quais tenha declarado, mediante decisão, que asseguram ou não um nível de proteção adequado.

5 CONSIDERAÇÕES FINAIS

A recolha e partilha de dados de caráter pessoal aumentaram exponencialmente nos últimos anos. Numa economia cada vez mais baseada em dados é impensável um mundo sem fluxos transfronteiriços de informação. O caráter crescente das transferências de dados pessoais exige um reforço, em âmbito global, do direito à proteção de dados. Demanda quadros internacionais eficazes e interoperáveis sustentados em princípios universais firmes, que por um lado assegurem um elevado nível de proteção deste direito e, por outro, não imponham restrições desnecessá-

rias ao comércio e cooperação internacionais. Para que isto seja possível é necessário que se construam pontes entre os vários sistemas jurídicos – nacionais e regionais – de proteção destes dados. As decisões de adequação, no plano europeu, têm um claro potencial para desempenhar um papel importante na construção desses pontos de conexão entre os vários sistemas jurídicos. Além disso, este instrumento oferece, quer aos operadores econômicos, quer aos indivíduos, um maior nível de segurança relativamente aos países que se considera com uma proteção adequada. Por isso, a decisão de adequação em âmbito europeu deve ser priorizada sempre que estejam presentes as condições adequadas.

O acórdão *Schrems,* ao esclarecer que o princípio do nível de proteção adequada exige ao país terceiro assegurar, efetivamente, um nível de proteção das liberdades e direitos fundamentais *substancialmente equivalente* ao conferido dentro da UE, permite uma flexibilidade aos meios a que esse país pode recorrer para assegurar tal nível de proteção. Desta forma, preserva-se uma certa margem de abertura para adaptar as apreciações de adequação às diferentes culturas e tradições jurídicas. Ao mesmo tempo reforça-se o direito à proteção de dados pessoais – tal como está protegido na Carta dos Direitos Fundamentais – ao exigir que se garanta o mesmo nível de proteção que esses dados obtêm dentro da UE.

Por outro lado, tanto o acórdão *Schrems* como o novo Regulamento esclarecem que a avaliação de adequação incide não apenas sobre a legislação e as práticas relacionadas com a proteção de dados pessoais para fins comerciais e privados mas, também, sobre todos os aspectos do quadro aplicável a esse país, tais como: a segurança nacional e o respeito dos direitos fundamentais. Por último, sublinha-se que os mecanismos de controle da eficácia das decisões de adequação previstos no novo Regulamento vêm preencher uma notória lacuna e podem desempenhar um papel importante no aumento da eficácia destas decisões.

O escasso número de decisões de adequação no plano europeu, assim como o fracasso da eficácia dos princípios de porto seguro na proteção dos dados, são aspectos que têm minado o claro potencial destas decisões, no entanto, quer as clarificações do acórdão *Schrems,* quer as novidades introduzidas pelo novo quadro jurídico europeu para as transferências internacionais de dados pessoais podem transformar-se em dois importantes aliados para um novo impulso na adoção das decisões de adequação.

6 REFERÊNCIAS

AGÊNCIA EUROPEIA DOS DIREITOS FUNDAMENTAIS DA UNIÃO EUROPEIA; CONSELHO DA EUROPA. *Manual da Legislação Europeia sobre Proteção de Dados.* 2. ed. Luxemburgo: Serviço de Publicações da União Europeia, 2014.

RODRIGUES ARAÚJO, A.; OLIVEIRA, J. As transferências de dados pessoais para países terceiros acompanhada de uma decisão de adequação no direito da União Europeia. *Direito e Novas Tecnologias I.* CONGRESSO NACIONAL DO COMPEDI/UFPB, 33., Florianópolis: Compedi, 2014. p. 282-308.

AUTORIDADE EUROPEIA PARA A PROTEÇÃO DE DADOS. AEPD. *Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions – A comprehensive approach on personal data protection in the European Union.* 2011. Disponível em: <http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf>. Acesso em: 13 jun. 2016.

_____. *The transfer of personal data to third countries or international organizations by EU institutions and bodies.* 2014. Disponível em: <https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Papers/14-07-14_transfer_third_countries_EN.pdf>. Acesso em: 13 jun. 2016.

COMISSÃO EUROPEIA. *Relatório da Comissão:* primeiro relatório sobre a implementação da directiva relativa à protecção de dados (95/46/*CE)*. 2003. Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex:52003DC0265>. Acesso em: 13 jun. 2016.

_____. *Special Eurobarometer 431:* Data Protection. 2015a. Disponível em: <http://ec.europa.eu/public_opinion/archives/ebs/ebs_431_en.pdf>. Acesso em: 13 jun. 2016.

_____. *Communication from the Commission to the European Parliament and the Council on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14 (Schrems)*. 2015b. Disponível em: <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52015DC0566>. Acesso em: 13 jun. 2016.

FERRETTI, F. Data Protection and the legitimate interest of data controllers: much ado about nothing or the winter of rights*? Common Market Law Review*, Reino Unido, v. 51, n. 3, p. 843-868, 2014.

FLORIDI, L. The Informational Nature of Personal Identity. *Mindes & Machines: Journal of Artificial Intelligence, Philosophy and Cognitive Science*, v. 21, n. 4, p. 549-566, 2011.

FUSTER, G.; SCHERRER, A. *Big Data and Smart Devices and Their Impact on Privacy:* Study for the LIBE Committee: European Union. Bruxelas: Serviço de Publicações da União Europeia, 2015.

GILBERT, F. European Data Protection 2.0: New Compliance Requirements in Sight – What the Proposed EU Data Protection Regulation Means for U.S. Companies. *Santa Clara Computer & Hight Tech L. J.*, v. 28, n. 4, p. 815-863, 2012.

GRUPO DE TRABALHO DO ARTIGO 29. *Primeiras orientações sobre as transferência de dados pessoais para países terceiros* – eventual metodologia a adoptar para avaliar a adequação do grau de proteção. 1997. Disponível em: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm>. Acesso em: 13 jun. 2016.

GRUPO DE TRABALHO DO ARTIGO 29. *Transferência de dados pessoais para países terceiros:* aplicação dos artigos 25 e 26 da Directiva Comunitária relativa à proteção de dados. 1998. Disponível em: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm>. Acesso em: 13 jun. 2016.

GRUPO DE TRABALHO DE PROTEÇÃO DE DADOS DO ARTIGO 29. *Parecer 4/2007 sobre o conceito de dados pessoais*. 2007. Disponível em: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm>. Acesso em: 13 jun. 2016.

GUMZEJ, N. Data protection for the digital age: comprehensive effects of the evolving law of accountability. *Juridical Tribune,* v. 2, n. 2, p. 82-108, 2012.

HOEREN, T. Information Management abd Data Protection within the EC-the amended EC proposal for a council directive on data protection and its impact on German industry. *International Journal of Law and Technology*, v. 1, n. 2, p. 129-143, 1993-1994.

HUSTINX, P. *EU Data Protection: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation*. 2015. Disponível em: <https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2014/14-09-15_Article_EUI_EN.pdf>. Acesso em: 13 jun. 2016.

KUNER, C. *Transborder Data Flows and Data Privacy Law.* Oxford: Oxford University Press, 2013.

_____. Reality and Illusion in EU Data Transfer Regulation Post Schrems. *Legal Studies Research:* Paper Series. Cambridge: University of Cambridge. Paper n. 14/2016, 2016.

MANGAS MARTÍN, A. Artículo 52: Comentário. In: MANGAS MARTÍN, M. (Org.). *Carta de los derechos Fundamentales de la Unión Europea:* comentário artículo por artículo. Madrid: Fundación BBVA, 2008. p. 826-851.

PARLAMENTO EUROPEU. *Resolução do Parlamento Europeu, de 6 de Julho de 2011, sobre uma abordagem global da protecção de dados pessoais na União Europeia*. 2011. Disponível em: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2011-0323+0+DOC+XML+V0//PT>. Acesso em: 13 jul. 2016.

_____. *Resolução do Parlamento Europeu de 12 de março de 2014, sobre a vigilância da Agência Nacional de Segurança dos EUA (NSA), os organismos de vigilância em diversos Estados-Membros e o seu impacto nos direitos fundamentais dos cidadãos da EU e na cooperação transatlântica no domínio da justiça e dos assuntos internos.* 2014. Disponível em: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0230+0+DOC+XML+V0//PT>. Acesso em: 13 jun. 2016.

_____. *Resolução do Parlamento Europeu, de 26 de maio de 2016, sobre a transferência transatlântica de dados.* 2016. Disponível em: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2016-0233+0+DOC+XML+V0//PT&language=PT>. Acesso em: 13 jun. 2016.

RODRIGUES ARAÚJO, A.; OLIVEIRA, J. As transferências de dados pessoais para países terceiros acompanhada de uma decisão de adequação no direito da União Europeia. *Direito e Novas Tecnologias I*. CONGRESSO NACIONAL DO COMPEDI/UFPB, 33. Florianópolis: Compedi, 2014.

SCHWARTZ, P. European Data Protection Law and Restrictions on International Data Flows. *Iowa Law Review,* v. 80, p. 471-495, 1994-1995.

WARREN, S.; BRANDEIS, L. The right to privacy. *Harvard Law Review,* v. 4, p. 193-220, 1890.

ZINSER, A. European Data Protection Directive: The Determination of the Adequacy Requirement in International Data Transfers. *Tulane Journal of Technology and Intellectual Property*, v. 6, p. 171-179, Spring 2004.

Legislação e Tratados

Comitê Misto do EEE. *Decisão do nº 83/1999 de 25 de junho de 1999 que altera o Protocolo nº 37 e o anexo IX* (serviço de telecomunicações do Acordo EEE) (JO L 296 de 23.11. 2000, p. 41).

União Europeia. *Carta dos Direitos Fundamentais da União Europeia* (JO C de 26.20.2012, p. 391).

União Europeia. *Decisão da Comissão de 30 de junho de 2003 nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de proteção dos dados pessoais na Argentina* (C(2003)1731 final de 30.6.2003).

União Europeia. *Decisão de execução da Comissão de 21 de agosto de 2012 nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de proteção de dados pessoais pela República Oriental do Uruguai no que se refere ao tratamento automatizado de dados* (JO L 215 de 25.8.2000, p. 1).

União Europeia. *Decisão-Quadro 2008/977/JAI do Conselho, de 27 de novembro de 2008, relativa à proteção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal aplica-se para a proteção de dados pessoais nestas matérias* (JO L 350 de 30.12.2008, p. 60).

União Europeia. *Diretiva 95/46/CE do Parlamento Europeu e do Conselho de 24 de outubro de 1995 relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre-circulação desses dados* (JO L 281 de 23.11.1995, p. 31)

União Europeia. *Diretiva 2002/58/CE do Parlamento Europeu e do Conselho de 12 de julho de 2002 relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações electrônicas* (JO L 201 de 31.7.2002, p. 37).

União Europeia. *Regulamento (CE) n□ 45/2001 do Parlamento Europeu e do Conselho, de 18 de dezembro de 2000, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre-circulação desses dados* (JO L 8 de 12.1.2001, p. 1).

União Europeia. *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre-circulação desses dados e que revoga a Diretiva 95/46/CE* (JO L 119 de 4.5.2016, p. 1).

União Europeia. *Tratado da União Europeia* (JO C 326 de 26.10.2012, p. 13).

União Europeia. *Tratado sobre o Funcionamento da União Europeia* (JO C 326 de 26.10.2012, p. 47).

Jurisprudência

TJUE, Acórdão de 6 de novembro de 2003, processo C-101/01, *Göta hovrat* c. *Bodil Lindqvist*.

TJUE, Acórdão de 8 de abril de 2014, processos apensos C-293 e C-594/12, *Digital Rights Ireland Ltd c. Minister for Communications e Outros,*

TJUE, Acórdão de 13 de maio de 2014, processo C-131/12, *Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González.*

TJUE, Acórdão de 6 de outubro de 2015, processo C-362/14, *Maximilian Schrems* c. *Data Protection Commissioner.*

Recebido em: 13/6/2016

Revisões requeridas em: 28/11/2016

Aceito em: 28/12/2016