HERACLIDES SEQUEIRA DOS SANTOS SILVA

A PROTECÇÃO DE DADOS PESSOAIS NA ERA GLOBAL: O CASO SCHREMS

Dissertação com vista à obtenção do grau de Mestre em Direito,
na área de Ciências Jurídicas Forenses.

Orientador:
Doutor Francisco Pereira Coutinho, Professor da Faculdade de Direito da Universidade Nova de Lisboa

Janeiro de 2017

HERACLIDES SEQUEIRA DOS SANTOS SILVA

A PROTECÇÃO DE DADOS PESSOAIS NA ERA GLOBAL: O CASO SCHREMS

Dissertação com vista à obtenção do grau de Mestre em Direito,
na área de Ciências Jurídicas Forenses.

Orientador:
Doutor Francisco Pereira Coutinho, Professor da Faculdade de Direito da Universidade Nova de Lisboa

Janeiro de 2017

Declaração de Compromisso de Anti-Plágio

Declaro por minha honra que o trabalho que apresento é original e que todas as minhas citações estão correctamente identificadas. Tenho consciência de que a utilização de elementos alheios não identificados constitui uma grave falta ética e disciplinar.

Lisboa, 5 de Janeiro de 2017

_____

(Heraclides Sequeira dos Santos Silva)

AGRADECIMENTOS

A realização da presente tese não teria sido possível sem o apoio de diversos amigos, familiares e colegas, sendo agora o momento certo para fazer o devido reconhecimento.

Antes de mais, um agradecimento muito especial ao Professor Francisco Pereira Coutinho, cujas sugestões de temas e de bibliografia foram essenciais para que pudesse redigir uma tese de mestrado sobre uma matéria que sempre me fascinou.

À minha família e amigos, que me deram todo o apoio necessário para que a escrita desta tese fosse o menos custosa possível.

Por fim, mas não menos importante, agradeço aos meus pais por toda a ajuda prestada, a quem espero um dia poder compensá-los por tanta generosidade.

MODOS DE CITAR E OUTROS ESCLARECIMENTOS

1. As monografias são citadas da seguinte forma: autor, título integral da obra, volume, edição, editora, local de publicação, ano de publicação e página que se pretende referenciar.

2. Os artigos constantes de livros ou de publicações periódicas são citados do seguinte modo: autor, título do artigo, livro ou publicação periódica, local, volume e/ou número da publicação, ano de publicação e páginas.

3. Quanto as obras ou artigos tenham sido consultados e recolhidos na Internet, a forma de citação será a seguinte: autor, título do artigo, nome do *site* em que foi obtido, data da publicação, endereço electrónico e data da consulta.

4. Nas publicações da autoria de uma instituição, o nome desta vem no lugar do autor.

5. É usado o modo itálico para destacar as palavras escritas em língua estrangeira e latinismos.

6. Declara-se que o corpo da presente tese de mestrado, incluindo espaços e notas, ocupa um total de 197.984 caracteres.

7. Informa-se ainda que a presente tese foi redigida conforme as regras do antigo Acordo Ortográfico.

LISTA DE SIGLAS E ABREVIATURAS

AEPD – Autoridade Europeia para a Protecção de Dados

Al. – Alínea

Art. – Artigo

Arts. – Artigos

Carta – Carta dos Direitos Fundamentais da União Europeia

Convenção 108 – Convenção para a Protecção das Pessoa relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal do Conselho da Europa

Directiva – Directiva 95/46/CE, de 24 de Outubro de 1995

N.º – Número

P. – Página

Pp. – Páginas

UE – União Europeia

EUA – Estados Unidos da América

Regulamento – Regulamento (UE) n.º 679/2016, de 27 de Abril de 2016 (Regulamento Geral sobre a Protecção de Dados)

RESUMO

Com o título “A Protecção de Dados Pessoais na Era Global: o Caso Schrems”, a presente tese tem como objectivo analisar as dificuldades que acarreta a construção de um quadro jurídico para as transferências transatlânticas de dados pessoais que esteja conforme aos requisitos europeus de protecção de dados pessoais e de respeito pela privacidade e vida familiar.

Proferido pelo Tribunal de Justiça a 6 de Outubro de 2015, o Acórdão Schrems marcou uma viragem nas relações comerciais entre a União Europeia e os Estados Unidos, ao declarar como inválida a intitulada Decisão “Porto Seguro”, que até então permitia a livre circulação de dados pessoais da União Europeia para as empresas norte-americanas que subscrevessem os princípios que tinham sido previamente definidos na decisão de adequação da Comissão Europeia. Pela sua importância, este acórdão será o ponto de partida do estudo a realizar neste trabalho.

Numa época em que as transferências de dados adquiriram um papel determinante na economia internacional, fruto do desenvolvimento tecnológico, as autoridades europeias e norte-americanas conceberam um novo quadro jurídico que substituísse o mecanismo precedente, ao qual deram a designação de “Escudo de Protecção da Privacidade UE-EUA”. Contudo, surgiram várias críticas ao pacto alcançado, afirmando que este mantinha os mesmos elementos que determinaram a invalidação da Decisão “Porto Seguro”, o que contraria as exigências expressas no Acórdão Schrems e cria a possibilidade de o novo quadro normativo ser novamente declarado inválido pelo Tribunal de Justiça.

Com base na investigação que será feita ao longo da tese aos motivos que justificaram a declaração de invalidade da Decisão “Porto Seguro”, bem como aos que fundamentam os receios de que o “Escudo de Protecção da Privacidade UE-EUA” tenha o mesmo fim, seremos capazes de responder à seguinte pergunta: será que se pode qualificar o “Escudo de Protecção da Privacidade UE-EUA” como um quadro jurídico viável para as transferências transatlânticas de dados pessoais?

Palavras-chaves: Protecção de Dados Pessoais; Schrems; Decisão "Porto Seguro"; "Escudo de Protecção da Privacidade UE-EUA"; União Europeia; Transferência de Dados Pessoais para Países Terceiros; Estados Unidos da América.

ABSTRACT

Entitled "The Protection of Personal Data in the Global Era: The Schrems Case ", this thesis is an analysis of the difficulties that entails the creation of a framework for transatlantic data transfers that conforms with the European requirements for personal data protection and the respect for privacy and family life.

Adopted by the Court of Justice on 6th October 2015, the *Schrems* Case marked a turning point in trade relations between the European Union and the United States by declaring invalid the “Safe Harbor" Decision, which until then allowed the free movement of personal data from the European Union to the United States. Due to its importance, the Court of Justice’s judgement will be the starting point of this thesis.

At a time when data transfers acquired a leading role in the international economy, European and North-American officials devised a new legal framework to replace the previous mechanism and gave it the name “EU-U.S. Privacy Shield". However, there were several criticisms to this agreement. Most stated that it maintained the same elements that led to the invalidation of the “Safe Harbor" Decision. The possibility of this agreement being declared invalid by the Court of Justice is real.

Based on the research which is going to be done in this thesis about the reasons that made invalid the “Safe Harbor” Decision, as well as the reasons which justify the fears that the “EU-U.S Privacy Shield” has the same end, we are going to be able to answer the following question: should we qualify the “EU-U.S. Privacy Shield” as a viable legal framework for transatlantic data flows?

Key words: Personal Data Protection; Schrems; “Safe Harbor" Decision; “EU-U.S Privacy Shield”; European Union; Transfer of Personal Data to Third Countries; United States of America.

1. INTRODUÇÃO

1. Devido à evolução das novas tecnologias de informação e comunicação e ao seu impacto no desenvolvimento económico e social, decorrente do processo de globalização, a UE teve que adoptar um novo paradigma em que a informação, entendida como o conhecimento de uma realidade, assume uma importância vital para a actividade económica e para o bem-estar social. [1]

Constituída por tratados internacionais de tipo clássico, a UE consiste numa associação permanente de Estados soberanos, fundada para a prossecução de objectivos comuns aos membros que a compõem. Para o efeito, é habilitada de órgãos próprios que exprimem, em conformidade com as regras estabelecidas, a sua vontade, sendo esta juridicamente distinta da dos Estados-Membros.[2] Enquanto organização internacional supranacional, a UE distingue-se pela originalidade de ter a capacidade de adoptar medidas que podem colocar em causa os direitos fundamentais dos cidadãos europeus.

A aquisição, armazenamento, tratamento e transmissão da informação, quando esta seja considerada relevante para a satisfação das necessidades das empresas e dos cidadãos, desempenha um papel determinante neste novo modelo de sociedade, a que muitos designam de "sociedade de informação", e à qual os Estados que fazem parte da UE não ficaram alheios.

Para que se adaptassem a essa nova realidade, a Comissão Europeia, enquanto principal órgão de direcção e execução da UE, viu-se na necessidade de avançar com a celebração de acordos com países que não fazem parte do espaço europeu, a fim de estabelecer uma base legal comum que permita o intercâmbio de informações, fortalecendo, assim, as trocas comerciais e a cooperação internacional com a parte contrária do acordo.

---

[1] COMISSÃO EUROPEIA, "Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões - Para uma economia dos dados próspera", COM(2014) 442 final, Bruxelas, 2 de Julho de 2014.

[2] CAMPOS, João Luiz Mota de, CAMPOS, João Mota de, *Manual de Direito Europeu - O sistema institucional, a ordem jurídica e o ordenamento económico da União Europeia*, 7.ª edição, Coimbra Editora, 2010, p. 65.

No entanto, muitos questionaram a capacidade dos acordos celebrados em garantir a defesa dos dados pessoais[3] dos cidadãos europeus de qualquer acesso ou uso ilegítimo, num momento em que os meios disponíveis para tal são vastos e de fácil utilização, em virtude do desenvolvimento tecnológico.

2. Tendo como título "A Protecção de Dados Pessoais na Era Global: o Caso Schrems", a presente tese consiste numa análise à problemática da construção de um quadro jurídico para os fluxos transatlânticos de dados pessoais que corresponda às exigências do direito da UE em matéria de protecção de dados pessoais e respeito pela vida privada. As questões jurídicas que o estabelecimento de tal quadro suscita, motivadas essencialmente pela divergência entre as legislações europeia e norte-americana do grau de protecção conferido aos dados pessoais, serão igualmente objecto de análise.

Como o subtítulo da própria tese indica, o ponto de partida do estudo será o Acórdão Schrems.[4] Proferido a 6 de Outubro de 2015 pelo Tribunal de Justiça da União Europeia, este acórdão teve como principal consequência a invalidação da Decisão "Porto Seguro" (*Safe Harbour Decision*) [5], que até então regulava as transferências de dados pessoais da UE para as organizações norte-americanas que subscrevessem os princípios consagrados no anexo I da referida decisão. [6]

---

[3] Por "dados pessoais", entende-se qualquer "informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, directa ou indirectamente, em especial por referência a um identificador" (art. 4.º, n.º 1, do Regulamento Geral sobre a Protecção de Dados, cuja definição é idêntica à do art. 2.º, *a*), da Directiva 95/46/CE).

[4] Acórdão *Maximillian Schrems vs. Data Protection Commissioner* do Tribunal de Justiça da União Europeia, de 6 de Outubro de 2015, do processo C‑362/14. Disponível em http://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:62014CJ0362&from=EN (data da consulta: 05-01-2017).

[5] Decisão 2000/520/CE da Comissão, de 26 de Junho de 2000, nos termos da Directiva 95/46/CE do Parlamento Europeu e do Conselho e relativa ao nível de protecção assegurado pelos princípios de «porto seguro» e pelas respectivas questões mais frequentes (FAQ) emitidos pelo *Department of Commerce* dos Estados Unidos da América, *Jornal Oficial das Comunidades Europeias*, 25 de Agosto de 2000. Pp. 7 – 47.

[6] Anexo I da Decisão 2000/520/CE da Comissão, de 26 de Junho de 2000, referente aos princípios de "porto seguro" (protecção da vida privada), emitidos pelo *Department of Commerce* dos EUA em 21 de Julho de 2000, *Jornal Oficial das Comunidades Europeias*, 25 de Agosto de 2000. Pp. 10 – 12.

Dada a importância que essa decisão da Comissão teve para as relações comerciais entre os dois lados do Atlântico, as autoridades europeias e norte-americanas iniciaram um período de negociações para encontrar uma solução que correspondesse, de igual modo, às necessidades de uma economia cada vez mais global e às condições estabelecidas no Acórdão Schrems para a adopção de um novo quadro para as transferências de dados pessoais dos cidadãos europeus.

Dessas negociações resultaram o "Escudo de Protecção da Privacidade UE-EUA" (*EU-U.S. Privacy Shield*), aprovado a 12 de Julho de 2016.[7] Não obstante os comentários positivos que recebeu por parte das empresas do sector das tecnologias e comunicação,[8] o acordo alcançado foi criticado pelo Schrems[9] e por vários organismos europeus[10] por persistir nos mesmos elementos que levaram à revogação do mecanismo precedente, contrariando as indicações expressas no Acórdão Schrems.

3. Estabelecido o âmbito de estudo deste trabalho, importa especificar os objectivos e a estrutura da presente tese. Os objectivos a prosseguir são os seguintes:

- Identificar as normas europeias que regulam os fluxos transfronteiriços de dados pessoais;

- Conhecer o funcionamento e a estrutura da Decisão "Porto Seguro", bem como as críticas que lhe foram feitas durante a sua vigência;

---

[7] *Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield.* Disponível em http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf (data da consulta: 05-01-2017).

[8] Neste sentido, e a mero título de exemplo, *Microsoft's commitments, including DPA cooperation, under the EU-U.S. Privacy Shield*, 11 de Abril de 2016. Disponível em https://blogs.microsoft.com/eupolicy/2016/04/11/microsofts-commitments-including-dpa-cooperation-under-the-eu-u-s-privacy-shield/ (data da consulta: 05-01-2017).

[9] EUROPE VERSUS FACEBOOK*, Privacy Shield – Press Breakfast by MEP Jan Albrecht (Statement by Max Schrems, Summary)*, Bruxelas, 12 de Julho de 2016. Disponível em http://www.europe-v-facebook.org/PA_PS.pdf (data da consulta: 05-01-2017).

[10] Entre os quais, o Grupo de Trabalho do Art. 29: *Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision*, Bruxelas, 13 de Abril de 2016. Disponível em http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf (data da consulta: 05-01-2017).

- Analisar os argumentos do TJUE que justificaram a declaração de invalidade da Decisão "Porto Seguro" no Acórdão Schrems;

- Compreender o impacto que o Acórdão Schrems teve nas relações transatlânticas;

- Dar a conhecer os instrumentos jurídicos alternativos para as transferências de dados pessoais da UE para os Estados Unidos (doravante, «EUA»);

- Descrever o processo de formação e o conteúdo do "Escudo de Protecção da Privacidade UE-EUA";

- Elencar as reacções que o "Escudo de Protecção da Privacidade UE-EUA" obteve das empresas da indústria das tecnologias e comunicações, de Schrems e das instituições europeias incumbidas de darem o seu parecer sobre o projecto de decisão de adequação do novo acordo;

- Reflectir sobre as consequências da adopção do "Escudo de Protecção da Privacidade UE-EUA" e os possíveis desenvolvimentos futuros.

Tendo em consideração esses objectivos, foi definida a seguinte questão de investigação:

- Será que se pode qualificar o "Escudo de Protecção da Privacidade UE-EUA" como um quadro jurídico viável para as transferências transatlânticas de dados pessoais, tendo em conta os critérios estabelecidos pelo TJUE no Acórdão Schrems e as críticas que recebeu?

4. A tese está organizada em oito capítulos. O Capítulo 1 é constituído pela presente introdução, na qual são traçados o âmbito do estudo, os objectivos e as questões de investigação.

No Capítulo 2 será descrito o processo de formação do regime jurídico europeu de protecção de dados pessoais, tanto a nível do Conselho da Europa como a da UE. Da legislação europeia para a protecção de dados, será dada uma especial atenção ao estudo das regras que regulam os fluxos

transfronteiriços de dados. Os instrumentos alternativos que podem ser utilizados para a concretização desses fluxos serão igualmente analisados.

A reforma que as instituições europeias operaram sobre o regime jurídico de protecção de dados pessoais vem, no entanto, trazer alterações ao modo como se processa a transmissão e o tratamento dos dados dos cidadãos europeus. O Capítulo 2 terminará, portanto, com a análise a este novo regime.

No Capítulo 3, será explicada a Decisão "Porto Seguro", onde foi classificado como adequado o nível de protecção da transferência de dados a partir da UE para os EUA. A estrutura criada para possibilitar fluxos transatlânticos de dados em grande escala, bem como o seu modo de operação, serão tratados neste ponto da tese.

Na perspectiva das relações comerciais entre a UE e os EUA, a adopção da Decisão "Porto Seguro" foi recebida com entusiasmo, ainda que tenham surgiram dúvidas quanto à capacidade da Decisão "Porto Seguro". Estas duas visões sobre a mesma decisão serão explicadas no final do Capítulo 3.

O Capítulo 4 será dedicado ao Acórdão Schrems. Nesta sentença, o TJUE declarou a invalidade da Decisão "Porto Seguro". Todo o processo que culminou nesta sentença será descrito no Capítulo 4, bem como os factos que o antecederam e a decisão propriamente dita. Na terceira secção do segundo subcapítulo será feita uma síntese conclusiva em que daremos o nosso parecer sobre os argumentos avançados pelo TJUE para invalidar a decisão de adequação em estudo.

Ao anular a Decisão "Porto Seguro", o TJUE pôs termo à vigência do quadro jurídico que durante quinze anos legitimou os fluxos de dados para os EUA. As consequências e reacções que tal decisão provocou serão abordadas no terceiro subcapítulo do Capítulo 4.

A 12 de Julho de 2016, foi adoptado pela Comissão um novo quadro transatlântico para os fluxos de dados: o "Escudo de Protecção da Privacidade

UE-EUA". Por constituir uma nova etapa para as relações entre a UE e os EUA no domínio das transferências de dados, o Capítulo 5 ser-lhe-á dedicado.

Composto por uma decisão e sete anexos, o "Escudo de Protecção da Privacidade UE-EUA" pretende reflectir os requisitos estabelecidos no Acórdão Schrems. As obrigações e garantias previstas no novo acordo serão aprofundadas nos dois primeiros subcapítulos do Capítulo 5, bem como as diferenças com o mecanismo precedente e o processo de negociações que culminou na adopção do "Escudo de Protecção da Privacidade UE-EUA".

As empresas norte-americanas que queiram transferir dados no âmbito do quadro aprovado terão que cumprir os princípios de privacidade que constam no anexo II do "Escudo de Protecção da Privacidade UE-EUA" e que serão explorados no terceiro subcapítulo do Capítulo 5.

No âmbito do procedimento estabelecido, o "Escudo de Protecção da Privacidade UE-EUA" foi objecto de dois pareceres do Grupo de Trabalho do Art. 29.º e da AEPD, bem como de uma resolução adoptada pelo Parlamento Europeu. O conteúdo de tais textos será exposto detalhadamente nos três últimos subcapítulos do Capítulo 5.

A recepção crítica do "Escudo de Protecção da Privacidade UE-EUA" não foi, no entanto, unânime, tendo sido marcada pela disparidade de posições. As opiniões favoráveis e desfavoráveis à aprovação do novo acordo serão analisadas, respectivamente, no primeiro e segundo subcapítulo do Capítulo 6. Uma síntese conclusiva sobre esta controvérsia será feita no terceiro subcapítulo do Capítulo 6.

As conclusões constituem o último capítulo do trabalho, onde será apresentada uma síntese global dos resultados que se obteve com as respostas dadas às questões de investigação e com a concretização dos objectivos propostos para esta tese.

2. REGIME JURÍDICO EUROPEU DE PROTECÇÃO DE DADOS PESSOAIS

2.1. Antecedentes e Formação do Modelo Europeu

2.1.1. Protecção de Dados no Direito do Conselho da Europa

Um ano antes daquele que seria o primeiro passo do processo de integração europeia – a instituição da Comunidade Europeia do Carvão e do Aço, através do Tratado de Paris, em 1951 –, já o Conselho da Europa, enquanto organização de cooperação internacional vocacionada para a promoção dos ideais e princípios que sejam comuns a todos os seus membros e do progresso económico e social[11], dava um contributo importante para a defesa do direito à protecção de dados pessoais[12], através da assinatura da Convenção Europeia dos Direitos do Homem, em 1950. No art. 8.º deste documento, verifica-se o seu reconhecimento como parte integrante do direito ao respeito pela vida privada e familiar, pelo domicílio e pela correspondência, estabelecendo ainda as condições em que são permitidas ingerências das autoridades públicas dos países membros nos dados pessoais dos seus cidadãos.

Na década de 60, com o surgimento da tecnologia da informação, verificou-se uma crescente necessidade de formular regras mais pormenorizadas e actuais de salvaguarda dos dados pessoais. Com este propósito, o Comité de Ministros do Conselho da Europa adoptou diversas resoluções na década seguinte, visando a protecção desses perante os bancos electrónicos de dados no sector privado[13] e privado.[14]

---

[11] Art. 1.º da Convenção de Londres, de 5 de Maio de 1949, que instituiu o Conselho da Europa.

[12] O direito à protecção de dados pessoais é reconhecido ao nível internacional em vários instrumentos adoptados sob a égide da Organização das Nações Unidos, sendo na maioria dos casos como uma extensão do direito à privacidade. Neste sentido, ver o art. 12.º da Declaração Universal dos Direitos Humanos; o art. 17.º do Pacto Internacional sobre os Direitos Civis e Políticos; o Comentário Geral n.º 16 sobre o direito ao respeito da privacidade, família, domicílio e correspondência, e protecção da honra e reputação – art. 17.º; e as Directrizes Para a Regulação de Ficheiros Informatizados de Dados de Carácter Pessoal, adoptadas pela Resolução 45/95 da Assembleia Geral das Nações Unidas, de 14 de Dezembro de 1990.

[13] Resolução (73) 22 do Comité de Ministros do Conselho da Europa (1973), relativa à protecção da privacidade das pessoas singulares perante os bancos electrónicos de dados no sector privado, de 26 de Setembro de 1973.

Em 1981, foi aberta à assinatura a Convenção para a Protecção das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal do Conselho da Europa, destinada à protecção das pessoas fase ao tratamento automatizado de dados de carácter pessoal. Este continua a ser o único instrumento internacional juridicamente vinculativo para os Estados signatários no domínio da protecção de dados.

Com aplicação a todos os tratamentos de dados realizados tanto pelo sector público como pelo privado, incluindo os efectuados pelas autoridades policiais e judiciais, a Convenção 108 pretende proteger as pessoas de qualquer abuso que possa ocorrer com a recolha e tratamento de dados pessoais através da consagração de diversas garantias jurídicas, procurando ainda regular o fluxo transfronteiriço de dados.

A Convenção 108 foi ratificada por todos os Estados-Membros da UE. Posteriormente, os princípios gerais e as regras estabelecidas no Convenção foram desenvolvidos e contextualizados em várias recomendações adoptadas pelo Comité de Ministros do Conselho da Europa, prática que ainda se mantém.[15] Em 1999, a Convenção 108 foi alterada[16] para permitir a adesão da UE[17] e, dois anos depois, foi-lhe adicionado um protocolo com disposições sobre os fluxos transfronteiriços de dados para Estados não signatários, isto é, para países terceiros, e sobre o estabelecimento obrigatório de autoridades nacionais de controlo de protecção de dados. [18]

---

[14] Resolução (74) 29 do Comité de Ministros do Conselho da Europa (1974), relativa à protecção da privacidade das pessoas singulares perante os bancos electrónicos de dados no sector público, de 20 de Setembro de 1974.

[15] A título de exemplo: Recomendação CM/Rec(2016)1 do Comité de Ministros, relativa à protecção e promoção do direito à liberdade de expressão e ao direito à vida privada no que diz respeito à neutralidade da rede, de 13 de Janeiro de 2016; Recomendação CM/Rec(2015)5 do Comité de Ministros, relativa ao tratamento de dados pessoais no contexto do emprego, de 1 de Abril de 2015; Resolução CM/Rec(2012)4 do Comité de Ministros, relativa à protecção dos direitos humanos no que diz respeito aos serviços das redes sociais, de 4 de Abril de 2012.

[16] Alterações à Convenção para a Protecção das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal (STCE n.º 108) que permitem a adesão das Comunidades Europeias, adoptadas pelo Comité de Ministros a 15 de Junho de 1999.

[17] Não obstante a aprovação de alterações à Convenção 108 e o facto de a totalidade dos Estados-Membros da União Europeia ter rectificado a Convenção, a União Europeia não chegou a aderir.

[18] Protocolo Adicional à Convenção para a Protecção das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal, respeitante às autoridades de controlo e aos fluxos transfronteiriços de dados, n.º 181, de 8 de Novembro 2001.

2.1.2. Protecção de Dados no Direito da União Europeia

2.1.2.1. Directiva 95/46/CE

Ainda que de forma gradual, a UE procurou estabelecer um regime jurídico que assegurasse uma eficaz protecção dos dados pessoais e promovesse a sua transmissão dentro e fora do espaço da UE, dados os benefícios que a vigência de um regime com essas características acarretaria para a consolidação do projecto europeu e para o desenvolvimento económico.

Com a entrada em vigor da Directiva 95/46/CE, de 24 de Outubro de 1995, foi estabelecido um regime geral de protecção de dados no território europeu, sujeitando o tratamento de dados pessoais a critérios de necessidade, pertinência e não excessividade em função às finalidades prosseguidas e limitando, em termos genéricos, a sua conservação ao período necessário para a prossecução das finalidades para que os mesmos são recolhidos ou para que devem ser tratados posteriormente. Aliada à sua importância para a defesa de direitos fundamentais, esta Directiva foi também pensada para promover os fluxos de dados pessoais dentro da Comunidade Europeia, reforçando, desta forma, o mercado único.

Ao aprovar a Directiva, a Comissão procurou tornar equivalente, em todos os Estados-Membros, o nível de protecção dos direitos e liberdades dos cidadãos quanto esteja em questão o tratamento dos seus dados pessoais, garantindo, desta forma, um elevado nível de protecção no espaço europeu através da harmonização das legislações nacionais sobre a protecção de dados. Em consequência disso, os Estados-Membros dispunham de uma reduzida margem de manobra na aplicação da Directiva.

O seu âmbito de aplicação territorial era amplo, já que não se restringia aos Estados-Membros, incluindo de igual modo países que não fazem parte da UE mas que pertencem ao Espaço Económico Europeu: a saber, a Islândia, o Listenstaine e a Noruega. [19]

[19] Art. 126.º, n.º 1, do Acordo sobre o Espaço Económico Europeu, *Jornal Oficial das Comunidades Europeias,* n.º L 001, 3 de Janeiro de 1994, p. 30. A Directiva foi formalmente integrada naquele Acordo através da Decisão n.º 83/1999 do Comité Misto do Espaço

No entanto, e uma vez que a Directiva não era aplicável ao tratamento de dados pessoais no âmbito da cooperação policial e judiciária em matéria penal, o Conselho adoptou a Decisão-Quadro 2008/977/JAI, de 27 de Novembro de 2008, a fim de assegurar a protecção dos dados recolhidos ou tratados pelas autoridades competentes quando justificado por motivos de prevenção, investigação, detecção, repressão de infracções penais e execução de sanções penais. A hipótese de as instituições e órgãos da UE poderem proceder a uma utilização e tratamento de dados pessoais que infringisse as regras europeias de protecção de dados não foi excluída, pelo que, para acautelar o aparecimento ou a impunibilidade dessas situações, foi estabelecido o Regulamento (CE) n.º 45/2001 do Parlamento Europeu e do Conselho, de 18 de Outubro de 2000.

2.1.2.2. Carta dos Direitos Fundamentais da União Europeia

Quando se aborda o tema do regime jurídico europeu de protecção de dados, é incontornável referir a relevância da Carta dos Direitos Fundamentais da União Europeia, proclamada em Dezembro de 2000 e aonde estão concentrados todos os direitos civis, políticos, económicos e sociais dos cidadãos europeus que decorram das tradições constitucionais e das obrigações internacionais comuns aos Estados-Membros.

Inicialmente um documento político, a Carta tornou-se juridicamente vinculativa como direito primário da UE com a entrada em vigor do Tratado de Lisboa, a 1 de Dezembro de 2009 (art. 6.º, n.º 1, do Tratado da UE).

Na Carta, para além de ser garantido o respeito pela vida privada e familiar (art. 7.º), é reconhecido o direito à protecção de dados[20] (art. 8.º, n.º 1), elevando este à condição de direito fundamental no quadro do direito da UE. Por ter sido formulado vários anos após a adopção da Directiva, o art. 8.º da Carta deve ser interpretado no sentido de incorporar a legislação da UE sobre protecção de dados anteriormente existente.

Económico Europeu, de 25 de Junho de 1999, que alterou o Protocolo n.º 37 e o anexo XI (serviços de telecomunicações) do referido Acordo.

[20] Este direito é também reconhecido no art. 16.º, n.º 1, do Tratado do Funcionamento da UE.

Para que o tratamento de dados de carácter pessoal seja considerado lícito, deverão ser observados os requisitos especificados no art. 8.º, n.º 2, da Carta, sendo que estes se referem a princípios fundamentais da protecção de dados que serão analisados posteriormente. A fiscalização do cumprimento das regras previstas fica a cargo de uma autoridade independente, conforme consta no art. 8.º, n.º 3, da Carta.

2.1.2.3. Outros Textos Jurídicos

Contudo, ainda que a Directiva continuasse a ser o principal instrumento legislativo da União em matéria de protecção de dados, houve a necessidade de estabelecer disposições mais detalhadas e actuais, de modo a assegurar a necessária clareza na conciliação com outros interesses legítimos e a acompanhar a evolução tecnológica.

Um exemplo desse esforço da UE em dotar o seu ordenamento jurídico de instrumentos jurídicos adequados à resolução das questões surgidas com os novos avanços tecnológicos foi a Directiva 2002/58/CE, de 12 de Julho, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas.

Porém, alguns dos textos legislativos produzidos levantaram dúvidas quanto à sua conformidade com os direitos à privacidade e à protecção de dados pessoais, consagrados nos arts. 7.º e 8.º da Carta, e, por isso, foram considerados inválidos pelo TJUE. Tal foi o caso da Directiva 2006/24/CE, de 15 de Março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações, no Acórdão *Digital Rights Ireland,* de 8 de Abril de 2014. [21]

[21] Acórdão *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources* e outros e *Kärntner Landesregierung* e outros do Tribunal de Justiça da União Europeia, de 8 de Abril de 2014, dos processos apensos C-293/12 e C-594/12. Disponível em http://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=PT (data da consulta: 05-01-2017). Neste acórdão, o Tribunal declarou a invalidade da Directiva 2006/24/CE, por considerar que esta não oferecia garantias de que a conservação e utilização de dados de tráfego se regiam por critérios de proporcionalidade e necessidade, violando, assim, os arts. 7.º, 8.º, e 52.º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia. Para mais informações sobre o impacto deste acórdão, RAMALHO, David Silva, COIMBRA, José Duarte, "A declaração de invalidade da Diretiva 2006/24/CE: presente e futuro da

2.2. Princípios Fundamentais

Consagrados originalmente na Convenção 108, o elencar dos princípios fundamentais sobre protecção de dados consta de qualquer texto legislativo adoptado pela UE que diga respeito a essa temática, sob pena de ser declarado inválido pelas instâncias judiciais. Surgem igualmente na Directiva, onde são explorados de forma mais pormenorizada.

2.2.1. Princípio do Tratamento Lícito

Identificado tanto na Convenção 108 (art. 5.º, alíneas *a)* e *b)*) como na Directiva (art. 6.º, n.º 1, alíneas *a)* e *b)*), o princípio do tratamento lícito estabelece que o tratamento de dados só é lícito quando for legitimado por lei e tido como necessário para a prossecução de uma finalidade específica e legítima.

Partindo do pressuposto de que o tratamento de dados poderá constituir uma ingerência no exercício do direito ao respeito pela vida privada da pessoa em causa, essa intromissão terá que ser justificada pela prevalência dada a um interesse público identificado ou aos direitos e liberdades dos outros em detrimento do direito ao respeito pela vida privada, uma vez que este não é absoluto e, portanto, pode ser parcialmente restringido com base numa disposição do direito interno.[22] A ingerência terá ainda que corresponder a uma necessidade social imperiosa e ser proporcional ao objectivo legítimo pretendido, segundo a jurisprudência do Tribunal Europeu dos Direitos Humanos.[23]

2.2.2. Princípio da Especificação e da Limitação da Finalidade

O princípio da especificação e da limitação da finalidade (art. 5.º, al. *b)*, da Convenção 108 e art. 6.º, n.º 1, al. *b)*, da Directiva) estabelece uma relação de dependência da legitimidade do tratamento de dados pessoais com a finalidade concreta em que assenta a decisão de proceder à recolha e

---

regulação sobre conservação de dados de tráfego para fins de investigação, deteção e repressão de crimes graves", in *O Direito*, Coimbra, Ano 147.º – IV, 2015. Pp. 997 – 1046.

[22] Conforme resulta da leitura do art. 52.º, n.º 1, da Carta.

[23] A título de exemplo, Acórdão *Gillow c. Reino Unido* do Tribunal Europeu dos Direitos Humanos, de 24 de Novembro de 1986, série A, n.º 109, § 55.

tratamento dos dados. Por força deste princípio, o tratamento é restringido pelo fim que lhe é inicialmente atribuído, pelo que qualquer outra finalidade dada aos dados adquiridos exigirá sempre uma base legal autónoma.

Por se reconhecer que uma utilização excessiva ou irregular dos dados pessoais pode ter graves consequências no direito ao respeito pela vida privada do seu titular, foram consagrados três princípios relativos à qualidade dos dados que a entidade responsável pelo tratamento tem necessariamente de aplicar:

2.2.2.1. Princípio da Pertinência dos Dados

Previsto no art. 5.º, al. *c)*, da Convenção 108 e no art. 6.º, n.º 1, al. *c)*, da Directiva, determina que o tratamento tenha somente como objecto os dados que sejam considerados *"adequados, pertinentes e não excessivos"* no que concerne ao propósito para o qual são recolhidos e tratados posteriormente. Mais explicitamente, as categorias de dados seleccionadas têm que ser imprescindíveis à concretização do objectivo geral do tratamento, devendo o seu responsável limitar a recolha de dados às informações que sejam pertinentes para a finalidade prosseguida.

2.2.2.2. Princípio da Exactidão dos Dados

Previsto no art. 5.º, al. *d)*, da Convenção 108 e no art. 6.º, n.º 1, al. *d)*, da Directiva, consiste na ideia de que a entidade encarregada do tratamento não deve utilizar as informações pessoais que possui sem antes se certificar, com um grau razoável de certeza, que esses dados são exactos e estão actualizados. O dever de asseverar o rigor dos dados tem de ser analisado no contexto da finalidade do tratamento dos dados, visto que, por exemplo, poderão haver situações em que o principal motivo do tratamento seja o de documentar acontecimentos e, nesse caso, uma actualização dos dados armazenados seria contra-procedente.

2.2.2.3. Princípio da Limitação da Conservação dos Dados

Previsto no art. 5.º, al. *e)*, da Convenção 108 e no art. 6.º, n.º 1, al. *e),* da Directiva), determina que os dados pessoais devem ser *"conservados de forma*

a permitir a identificação das pessoas em causa apenas durante o período necessário para a prossecução das finalidades para que foram recolhidos ou para que são tratados posteriormente."[24] Alcançados esses fins, os dados pessoais deverão ser eliminados. No entanto, o art. 6.º, n.º 1, al. *e),* da Directiva prevê expressamente uma derrogação a este princípio, que consiste na conservação dos dados para fins históricos, estatísticos ou científicos, cabendo aos Estados-Membros, no seu direito interno, o estabelecimento de garantias apropriadas para esses casos.

2.2.3. Princípio do Tratamento Leal

Com o princípio do tratamento leal (art. 5.º, al. *a)*, da Convenção 108 e art. 6.º, n.º 1, al. *a)*, da Directiva), pretende-se regular a relação entre a entidade responsável pelo tratamento e o titular dos dados, submetendo o tratamento à obrigação de ser lícito e transparente, especialmente no que diz respeito às pessoas em questão. Assim, exige-se que quem proceda ao tratamento dos dados informe regularmente os indivíduos em causa sobre a utilização que está a ser dada às suas informações pessoais. Nos seus esclarecimentos, deve recorrer a uma linguagem acessível, de modo a assegurar que os titulares entendem devidamente de que forma os seus dados estão a ser usados. Por seu lado, os particulares têm o direito de poderem solicitar à entidade responsável pelo tratamento a confirmação sobre se os seus dados estão a ser tratados e, em caso afirmativo, quais é que estão nessa situação, uma vez que o tratamento dissimulado e secreto de dados é proibido,[25] salvo nos casos expressamente autorizados por lei.[26]

2.2.4. Princípio da Responsabilidade

Embora a Convenção 108 não lhe faça qualquer referência, o princípio da responsabilidade é estabelecido pelo art. 6.º, n.º 2, da Directiva como o reconhecimento da competência da entidade responsável pelo tratamento em implementar medidas que promovam a protecção de dados nas suas actividades, responsabilizando-se pela conformidade das suas operações de

[24] Art. 6.º, n.º 1, al. e), da Directiva 95/46/CE, de 24 de Outubro.
[25] Art. 12.º, al. a), da Directiva 95/46/CE.
[26] Art. 13.º, n.º 1, alíneas a) a g), da Directiva 95/46/CE.

tratamento com a legislação europeia sobre protecção de dados em vigor. Em função disto, de acordo com o Grupo de Trabalho do Art.º 29,[27] recai sobre a entidade responsável pelo tratamento a obrigação de disponibilizar às pessoas em causa e às autoridades de controlo, quando lhe seja exigido por lei ou solicitado directamente, a documentação que comprove a aplicação de medidas destinadas a assegurar a cumprimento das regras sobre protecção de dados.

2.3. Fluxos Transfronteiriços de Dados Pessoais

Por fluxos transfronteiriços de dados entende-se a transferência de dados pessoais para um país destinatário específico, no qual serão objecto de tratamento. Esta circulação de dados, para ser permitida, tem que obedecer às regras estabelecidas no art. 2.º do Protocolo Adicional à Convenção 108, cabendo também aos Estados-Membros da UE o cumprimento dos arts. 25.º e 26.º da Directiva.

A liberdade de circulação dos dados pessoais entre as Partes da Convenção 108 ou entre os Estados-Membros está consagrada tanto na Convenção 108 como na Directiva, ainda que com diferenças. Na Convenção 108, o livre fluxo de dados para uma Parte Contratante só pode ser restringido se a natureza especial dos dados assim o impuser (art. 12.º, n.º 3, al. *a)*) ou se a restrição for justificada para evitar que a transferência se subtraia às disposições legais internas em matéria de migração transfronteiriça de dados para países terceiros (art. 12.º, n.º 3, al. *b)*). Por seu lado, na Directiva, qualquer restrição ou proibição à livre circulação de dados entre os Estados-Membros, por motivos referentes à protecção de dados, não é permitida (art. 1.º, n.º 2).

Quando o destinatário dos dados seja um Estado ou uma organização que não seja Parte da Convenção 108, a transferência sem reservas pode ser permitida, desde que se reconheça que o destinatário em causa possui comprovadamente um nível adequado de protecção de dados. É o que prevê o art. 2.º, n.º 1, do Protocolo Adicional da Convenção 108, competindo ao

[27] GRUPO DE TRABALHO DO ART. 29.º, "Parecer 3/2010 sobre o princípio da responsabilidade", WP 173, Bruxelas, 13 de Julho de 2010.

legislador nacional definir os critérios pelos quais se deve reger a avaliação do nível de protecção de um país estrangeiro e a entidade encarregada dessa apreciação.

Para além de regular o livre fluxo de dados entre Estados-Membros, a Directiva contém igualmente disposições sobre os requisitos da livre transferência de dados pessoais para países terceiros fora da UE. De acordo com o art. 25.º, n.º 1, a transferência para países terceiros só poderá ocorrer quando o país em questão assegure um nível de protecção adequado.

Segundo o art. 25.º, n.º 6, da Directiva, a Comissão é competente para apreciar o nível de protecção de dados de um país terceiro, podendo considerá-lo adequado quando salvaguarde os direitos das pessoas singulares, por força do seu direito interno ou de compromissos internacionais assumidos.

Na apreciação que faz ao nível de protecção de um país terceiro, atende ainda a todas as circunstâncias que envolvam a transferência de dados, nas quais constam a sua natureza, a finalidade e a duração do(s) tratamento(s) projectado(s), os países de origem e destino final e as regras de direito gerais ou sectoriais que vigoram no país, assim como as regras profissionais e as medidas de segurança que são respeitadas nesse país (art. 25.º, n.º 2, da Directiva).

Para auxiliá-lo nessa função, consulta o Grupo de Trabalho do Art.º 29, cujo nome advém do número do artigo da Directiva que lhe serve de base jurídica.[28] Em resposta ao pedido da Comissão, o Grupo de Trabalho do Art.º 29 emitirá um parecer sobre o nível de protecção dos dados pessoais no país terceiro em questão, constituindo esta uma das suas principais competências (art. 30.º, n.º 1, al. *a)*, da Directiva).

Para além do exercício dessa função, o Grupo de Trabalho do Art.º 29 destaca-se ainda pelo seu contributo substancial para a interpretação dos arts. 25.º e 26.º da Directiva através do documento que adoptou a 24 de Julho de 1998, intitulado "Transferência de dados pessoais para países terceiros:

[28] No n.º 1 deste artigo, o Grupo de Trabalho do Art. 29.º é definido como *"um Grupo de protecção das pessoas no que diz respeito ao tratamento de dados pessoais"* com carácter *"consultivo"* e *"independente"*.

aplicação dos arts. 25º e 26º da Directiva comunitária relativa à protecção dos dados". [29] Neste documento, estipula que a avaliação da adequação do nível de protecção deve comportar uma análise da legislação em vigor no país terceiro e da eficácia dos meios que visam assegurar a sua aplicação, estabelecendo também um conjunto de princípios substantivos da protecção de dados e de requisitos processuais de aplicação, cuja observância entende ser necessária para se poder constatar a existência de uma protecção adequada.

Com base no parecer do Grupo de Trabalho do Art.º 29, a Comissão adopta uma decisão relativa à adequação do nível de protecção dos dados pessoais do país em causa, fundamentando-a nos considerandos do documento. Tal decisão terá efeito vinculativo, ou seja, o fluxo de dados para o país em causa não estará sujeito a posteriores procedimentos de controlo ou autorização perante as autoridades nacionais dos Estados-Membros. Isto quer dizer, portanto, que basta à Comissão a publicação da sua constatação no *Jornal Oficial da União Europeia* para que essa vigore em todo o espaço europeu. De referir ainda que a Comissão pode limitar a sua decisão à análise de partes da jurisdição de um país ou de temas concretos.[30]

2.3.1. Instrumentos Jurídicos Alternativos

Nos casos previstos no n.º 1 do art. 26.º da Directiva, a livre transferência de dados pessoais para países terceiros que não possuam um nível adequado de protecção é possível, constituindo os casos previstos derrogações à regra estabelecida da obrigatoriedade de uma constatação sobre o grau de protecção conferido aos dados no país estrangeiro em causa. Contudo, por se tratar de desvios à regra geral, têm que ser interpretadas restritivamente e em especial quando a base legal da transferência seja o

[29] Este documento está disponível em http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/1998/wp12_pt.pdf (data da consulta: 05-01-2017).

[30] Por exemplo, a Decisão 2002/2/CE, de 20 de Dezembro de 2001, relativa à adequação do nível de protecção proporcionado pela lei canadiana sobre dados pessoais e documentos electrónicos, é uma decisão adoptada pela Comissão que se restringe à apreciação da legislação comercial canadiana.

consentimento do titular dos dados, no seguimento do que foi expressado pelo Grupo de Trabalho do Art. 29.[31]

Nas relações em que se aplique o Protocolo Adicional à Convenção 108, a transferência de dados para um destinatário que não esteja sujeito à jurisdição de uma Parte na Convenção e em que o Estado ou organização em questão não assegure um nível de protecção considerado adequado poderá, não obstante isso, ser autorizada.

Para tal, será necessário que se verifique uma das seguintes condições: a transferência estar prevista no direito interno por ser essencial em virtude de interesses específicos da pessoa em causa ou de interesses legítimos prevalecentes de terceiros, particularmente interesses públicos; ou a pessoa responsável pela transferência apresentar garantias que sejam julgadas suficientes pelas autoridades competentes, segundo o direito interno (artigo 2.º, n.º 2, do Protocolo Adicional à Convenção 108).

O conteúdo das alíneas do art. 26.º, n.º 1, da Directiva tem bastantes semelhanças com o das disposições do Protocolo Adicional à Convenção 108. Por força dos termos que constam na Directiva, os interesses da pessoa em causa poderão justificar a livre migração de dados para um país terceiro se o titular consentir, de forma inequívoca, a exportação dos seus dados (al. *a)*) ou se for imprescindível para a execução de um contrato entre a pessoa em causa e o responsável pelo tratamento (al. *b)*), para citar duas das hipóteses previstas.

Além disso, o direito interno pode também instituir regimes jurídicos aplicáveis às transferências transfronteiriças de dados para países terceiros que não garantam um nível adequado de protecção de dados. Para que esses fluxos ocorram nestas circunstâncias, a pessoa responsável pelo tratamento terá que apresentar garantias adequadas em matéria de protecção de dados, devendo submetê-las à apreciação da autoridade de controlo competente. Ainda que este requisito só seja expressamente mencionado no art. 2.º, n.º 2,

[31] GRUPO DE TRABALHO DO ART. 29.º, "Documento de trabalho sobre uma interpretação comum do artigo 26.º, n.º 1, da Directiva 95/46/CE de 24 de Outubro de 1995", *Working Paper 114*, Bruxelas, 25 de Novembro de 2005.

al. *b)*, do Protocolo Adicional à Convenção 108, considera-se que o mesmo é aplicável de igual modo no quadro da Directiva.

As garantias de protecção da vida privada e dos direitos e liberdades fundamentais dos particulares, assim como do exercício desses mesmos direitos, que o responsável pelo tratamento terá que assegurar podem ser fornecidas por via de cláusulas contratuais que vinculem o exportador e o importador dos dados, sendo que estas abrangem cláusulas contratuais-tipo (art. 2.º, n.º 2, al. *b)*, do Protocolo Adicional à Convenção 108 e art. 26.º, n.º 2 e n.º 4, da Directiva) e, no que concerne às transferências entre diferentes entidades inseridas no mesmo grupo empresarial multinacional, regras vinculativas para as empresas autorizadas pelas autoridades de protecção de dados (art. 26.º, n.º 2, da Directiva).

Outra opção igualmente reconhecida, que permite a transferência de dados para um país que não assegure um nível razoável de protecção, é quando seja sustentada por uma das derrogações expressamente indicadas nas alíneas *a)* a *f)* do art. 26.º, n.º 1, da Directiva.

Comparativamente às decisões de adequação, que resultam de uma avaliação global do sistema do país terceiro em causa e abrangem, em princípio, a totalidade das transferências para esse sistema, estes instrumentos jurídicos aplicam-se apenas a fluxos de dados específicos e não estão necessariamente confinados a um país específico. Além disso, ao não existir uma decisão de adequação que possa ser invocada, os exportadores e importadores de dados pessoais que recorram a essas bases jurídicas alternativas têm a responsabilidade de certificarem de que as transferências obedecem aos requisitos da Directiva.

No que diz respeito à utilização das cláusulas contratuais-tipo nas transferências internacionais de dados pessoais, a Comissão aprovou, para facilitar o seu uso e em conformidade com o art. 26.º, n.º 4, da Directiva, quatro conjuntos de cláusulas contratuais-tipo que acatam os critérios do art. 26.º, n.º 2, da Directiva: dois relativos às transferências entre responsáveis pelo

tratamento de dados[32]; os outros dois, relativos às transferências entre um responsável pelo tratamento de dados e um subcontratante que actue sob instruções daquele.[33]

Em comum, todos esses conjuntos de cláusulas contratuais-tipo estipulam obrigações aos exportadores e importadores de dados, que incluem deveres relativos às medidas de segurança, à informação do titular dos dados na circunstância de serem transferidos dados sensíveis, à notificação ao exportador de dados dos pedidos de acesso pelas autoridades competentes em função da aplicação da lei dos países terceiros ou de qualquer acesso acidental ou não autorizado, assim como aos direitos dos titulares dos dados em matéria de acesso, rectificação e supressão dos seus dados pessoais. De acrescentar que também devem constar regras sobre a reparação do titular dos dados caso se verifiquem danos decorrentes de uma violação praticada por uma das partes das cláusulas contratuais-tipo.

Uma outra opção admitida pela Comissão para as transferências transatlânticas de dados pessoais são as regras vinculativas para as empresas, ou, como são designadas pelo Grupo de Trabalho do art. 29.º [34], as *binding corporate rules* (BCR) (art. 26.º, n.º 2, da Directiva). Este tipo de regras apenas pode servir de base às transferências efectuadas dentro do mesmo grupo empresarial.

Com o recurso às regras vinculativas para as empresas, os dados pessoais podem circular livremente entre as diversas entidades de um grupo empresarial que opere a nível internacional, garantindo-se o mesmo nível de protecção de dados em todo o grupo por via de um único conjunto de normas vinculativas e executórias. Para facilitar a sua utilização, o Grupo de Trabalho

---

[32] Decisão 2001/497/CE da Comissão, de 15 de Junho de 2001, e Decisão 2004/915/CE da Comissão, de 27 de Dezembro de 2004, que alterou a primeira.

[33] Decisão 2002/16/CE da Comissão, de 27 de Dezembro de 2001, aplicada apenas aos contractos celebrados antes de 15 de Maio de 2010, e Decisão 2010/87/UE da Comissão, de 5 de Fevereiro de 2010.

[34] GRUPO DE TRABALHO DO ART. 29.º, "Statement on the implementation of the judgement of the Court of Justice of the European Union of 6 October 2015 in the Maximilian Schrems v Data Protection Commissioner case (C-362-14)", Bruxelas, 16 de Outubro de 2015. Disponível em http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf (data da consulta: 05-01-2017).

do Art. 29.º redigiu os requisitos materiais e processuais, fundados nas normas europeias de protecção de dados, pelos quais as empresas se devem reger na elaboração dessas regras.[35]

À semelhança do que acontece com as cláusulas contratuais-tipo, aos particulares, cujos dados estejam a ser tratados por uma entidade do grupo, deve ser garantida a possibilidade de poderem reivindicar os seus direitos junto de uma autoridade de protecção de dados e/ou um tribunal de um Estado-Membro quando as regras vinculativas para as empresas do grupo sejam desrespeitadas. De referir ainda que as transferências de dados efectuadas com base nessas regras necessitam de ser autorizadas pela autoridade de protecção de dados do Estado-Membro a partir do qual a empresa pretende transferir dados.

Por fim, independentemente do uso de cláusulas contratuais-tipo e/ou de regras vinculativas para as empresas, os dados pessoais são passíveis de serem transferidos para uma entidade localizada num país terceiro sem um nível de protecção adequado desde que se enquadre numa das derrogações alternativas previstas no art. 26.º, n.º 1, da Directiva. A título de exemplo, refira-se os casos em que haja consentimento prévio inequívoco do titular dos dados à transferência pretendida (al. *a)*) ou quando a transferência seja essencial para a celebração ou execução de um contrato celebrado no interesse do titular dos dados entre o responsável pelo tratamento e um terceiro (al. *c)*).

2.4. Reforma sobre a Protecção de Dados

Devido aos progressos tecnológicos e à globalização, o modo de acesso, recolha e utilização dos dados pessoais sofreu profundas alterações, trazendo novos desafios para a protecção de dados, aos quais as regras europeias em vigor não conseguem dar uma resposta satisfatória. Além disso, a divergência da transposição pelos Estados-Membros das normas europeias para o direito interno revela-se algo problemática, uma vez que agrava os

[35] Ver GRUPO DE TRABALHO DO ART. 29.º, "Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules", WP 153, 24 de Junho de 2008; "Working Document Setting up a framework for the structure of Binding Corporate Rules", WP 154, 24 de Junho de 2008; "Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules", WP 155 rev.04, 24 de Junho de 2008.

custos administrativos das empresas que pretendem actuar em todo o espaço europeu e dificulta a criação de um mercado único digital na Europa. [36]

A fim de actualizar e modernizar o regime vigente, a Comissão apresentou em Janeiro de 2012 um pacote de reforma sobre a protecção de dados. Com forte ênfase no reforço das regras internas da UE e na promoção de um maior controlo dos indivíduos sobre os seus dados, a reforma pretende pôr fim à fragmentação das normas de protecção de dados que se verifica actualmente na UE, garantindo, assim, a todos os cidadãos europeus o mesmo nível de protecção dos seus dados pessoais, independentemente do lugar em que estes forem tratados.

O pacote de reforma é composto por dois instrumentos jurídicos: o Regulamento Geral sobre a Protecção de Dados, que institui um quadro comum para a protecção de dados; a Directiva da Protecção de Dados destinados às autoridades policiais e judiciais.[37] Com o Regulamento, a Comissão procura eliminar as disparidades existentes no nível de protecção de dados entre os diferentes Estados-Membros, uma vez que o regulamento, devido à sua natureza, será directamente aplicável em todos os países que façam parte da UE. [38] Por seu turno, a Directiva da Protecção de Dados dirige-se a facilitar a cooperação transnacional da polícia ou do Ministério Público, de modo a tornar mais eficaz o combate contra a criminalidade ou o terrorismo na Europa.

Na sequência das negociações finais entre as instituições europeias, o Parlamento Europeu e o Conselho chegaram a um acordo político sobre o conjunto da reforma a 15 de Dezembro de 2015.[39] Partindo da modernização dos princípios estabelecidos na Directiva para a protecção de dados, o Regulamento foca-se no reforço dos direitos individuais e na consolidação do

[36] COMISSÃO EUROPEIA, "Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões - As plataformas em linha e o mercado único digital: Oportunidades e desafios para a Europa", COM(2016) 288 final, Bruxelas, 25 de Maio de 2016. P. 5. Disponível em http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52016DC0288&from=PT (data da consulta: 05-01-2017).
[37] Directiva (UE) 2016/680 do Parlamento Europeu e do Conselho de 27 de Abril de 2016, que revoga a Decisão-Quadro 2008/977/JAI do Conselho.
[38] Art. 288.º do Tratado de Funcionamento da UE.
[39] Art. 16.º, n.º 2, do Tratado de Funcionamento da UE.

mercado interno europeu, procurando ainda garantir uma aplicação mais rigorosa dos preceitos que regulam os fluxos transfronteiriços de dados pessoais.

Entre os diversos elementos que o constituem, o âmbito de aplicação territorial do Regulamento (art. 3.º, n.º 1 e n.º 2) é um dos mais relevantes, uma vez que as empresas sediadas num país terceiro que forneçam bens e serviços aos cidadãos europeus estão abrangidas pelas normas que nele constam. Ao sujeitar as empresas estrangeiras às mesmas regras a que estão submetidas as empresas estabelecidas na UE, garante-se que todas operem no espaço europeu em condições de concorrência equitativas, assegurando ainda que os direitos fundamentais das pessoas singulares da UE beneficiam do mesmo nível de protecção independentemente de onde esteja localizada a entidade que receba e trate dos seus dados pessoais. Esta aplicação extraterritorial do Regulamento constitui um dos maiores destaques da reforma efectuada ao regime europeu de protecção de dados, por ser suficiente que uma empresa proceda ao tratamento de dados pessoais de titulares residentes no território da União para estar vinculada ao cumprimento das normas que constam no Regulamento.

Correspondendo aos desejos dos cidadãos europeus em usufruírem de um maior controlo sobre as suas informações pessoais, os direitos dos indivíduos em matéria de protecção de dados são reforçados pelo Regulamento. O exercício do direito do titular em aceder aos seus próprios dados foi facilitado, sendo-lhe agora permitido obter informações mais completas sobre a utilização dada aos mesmos (art. 15.º). A portabilidade dos dados é igualmente consagrada como direito no Regulamento (art. 20.º), bem como a capacidade de solicitar o apagamento dos dados que lhe digam respeito ou, como é mais conhecido, o «direito a ser esquecido» (art. 17.º).

Para que as normas de protecção de dados previstas sejam efectivamente cumpridas pelas empresas que exerçam a sua actividade na UE, o Regulamento consagra um regime de sanções que harmoniza os poderes das autoridades nacionais de protecção de dados, habilitando estas a aplicar sanções dissuasivas às empresas que não respeitem as regras de protecção

de dados (art. 83.º, n.º 1 e n.º 2). Com este regime, as autoridades nacionais estarão habilitadas a aplicar coimas até 20 milhões de euros ou até 4 % do volume de negócios anual total de uma empresa (art. 83.º, n.º 6).

Ao sujeitar o tratamento de dados efectuado pelas autoridades policiais e judiciárias dos Estados-Membros ao cumprimento dos princípios e das regras gerais em matéria de protecção dos dados, a Directiva da Protecção de Dados contribui de forma determinante para uma melhor cooperação entre autoridades policiais e afins na aplicação coerciva da lei (art. 4.º, n.º 4). A inclusão na directiva de normas harmonizadas para as transferências internacionais de dados pessoais, no domínio da cooperação policial e judiciária em matéria penal, corroboram com essa ideia (art. 40.º).

No âmbito das investigações penais ou da aplicação das medidas de execução, o nível de protecção dos dados pessoais das vítimas, testemunhas e dos suspeitos de crimes sairá reforçado com a nova directiva (art. 12.º e seguintes). A supervisão cabe às autoridades nacionais independentes de protecção de dados (art. 41.º, n.º 1), devendo os particulares dispor de vias adequadas de recurso judicial (art. 52.º, n.º 1).

Não obstante manterem uma estrutura essencialmente idêntica à da Directiva, as normas que regulam as transferências de dados pessoais para países terceiros estão formuladas, tanto no Regulamento (art. 44.º e seguintes) como na Directiva da Protecção de Dados (art. 55.º e seguintes), de uma forma mais completa, transparente e pormenorizada, o que permite reduzir as formalidades administrativas e tornar mais rigorosa a aplicação das regras e excepções existentes.

Além disso, e em comparação com a Directiva, as disposições no Regulamento sobre a independência, funções e poderes das autoridades de protecção de dados da UE são definidas com mais detalhe (art. 51.º e seguintes). Nelas, está incluída explicitamente a possibilidade de suspender a transferência de dados para um destinatário num país estrangeiro ou para uma organização internacional (art. 58.º, n.º 2, al. *j)*). Por sua vez, a Directiva da Protecção de Dados contém normas idênticas sobre os fluxos transfronteiriços

(art. 35.º e seguintes) e os poderes das autoridades de protecção de dados no âmbito da aplicação coerciva da lei (art. 47.º).

Quanto às decisões de adequação da Comissão, onde esta avalia o nível de protecção de dados previsto na ordem jurídica de um país terceiro, o Regulamento estabelece uma lista pormenorizada dos elementos que a Comissão tem que necessariamente ter em conta na sua análise (art. 45.º, n.º 2), tais como o acesso das autoridades públicas aos dados pessoais (al. *a)*) ou a existência e o efectivo funcionamento de pelo menos uma autoridade de controlo independente no país terceiro ou à qual esteja sujeita uma organização internacional (al. *b)*).

Mais importante, contudo, é o facto de o Regulamento exigir expressamente que a Comissão reveja periodicamente todas as suas decisões de adequação (art. 45.º, n.º 3), de forma a garantir que toma conhecimento de qualquer alteração na situação de um país terceiro que possa ter repercussão sobre o nível de proteção conferido aos dados pessoais nessa ordem jurídica, o que implica um diálogo regular com as autoridades do país terceiro em causa.

No que se refere às transferências para países terceiros relativamente aos quais não tenha sido adoptada uma decisão sobre a adequação do nível de protecção, estão consagrados no Regulamento instrumentos alternativos para as transferências e as condições em que esses podem ser utilizados. Entre aqueles que prevê, constam as cláusulas contratuais-tipo (art. 46.º, n.º 2, alíneas *c)* e *d)*) e as regras vinculativas para empresas (art. 46.º, n.º 2, al. *b),* e art. 47.º), assim como os códigos de conduta aprovados e os mecanismos (art. 40.º e art. 46.º, n.º 2, al. *e)*) de certificação aprovados (art. 42.º e art. 46.º, n.º 2, al. *f)*).

Os textos legais que constituem o pacote da reforma da protecção de dados foram publicados a 4 de Maio de 2016 no *Jornal Oficial da UE.* Apesar de o Regulamento ter sido adoptado a 27 de Abril de 2016, só será aplicável a partir de 25 de Maio de 2018 (art. 99.º, n.º 2). Quanto à Directiva da Protecção de Dados, a sua entrada em vigor foi a 27 de Maio de 2016, devendo os

Estados-Membros transpô-la para o seu direito interno até 6 de Maio de 2018 (art.63.º, n.º 1).

Resumindo, com a aprovação desta reforma, as instituições europeias pretendem reforçar os direitos fundamentais dos cidadãos na era digital e facilitar a actividade comercial através da simplificação das leis aplicáveis, fortalecendo a confiança dos consumidores nos operadores europeus e estrangeiros e beneficiando, assim, o desenvolvimento digital a nível europeu e mundial.

3. DECISÃO "PORTO SEGURO" (*SAFE HARBOUR DECISION*)

3.1. Estrutura e Funcionamento

No contexto das decisões de adequação da Comissão sobre a adequação do nível de protecção de dados assegurado por um país terceiro, uma das mais relevantes foi a Decisão 520/2000/CE, designada como Decisão "Porto Seguro" (*Safe Harbour Decision*, no original).

Adoptada a 26 de Julho de 2000, reconhece, no seu art. 1º, n.º 1, que os princípios de "porto seguro", quando aplicados em conformidade com a orientação proporcionada pelas questões mais frequentes (FAQ) emitidas pelo Departamento do Comércio dos EUA em 21 de Julho de 2000, conferem um nível de protecção adequado às transferências de dados pessoais da UE para as organizações estabelecidas nos EUA.

Entre os princípios referentes à protecção da vida privada, que constam no anexo I da decisão, estão requisitos relativos à protecção dos dados pessoais, tais como os princípios de integridade dos dados, de segurança, de escolha e de retransferência. Constam igualmente na decisão padrões de conduta ao nível dos direitos concedidos aos titulares dos dados, como é o caso dos princípios de aviso, de acesso e de aplicação efectiva.

Essa decisão de adequação foi tomada na sequência dos pareceres do Grupo de Trabalho do Art. 29.º [40] e do Comité do Art. 31.º, tendo este último sido aprovado por maioria qualificada dos representantes dos Estados-Membros. Além disso, a Decisão "Porto Seguro" foi ainda submetida ao controlo prévio do Parlamento Europeu, em conformidade com o que é estabelecido pela Decisão 1999/468 do Conselho, de 28 de Junho de 1999, que define as regras de exercício das competências de execução atribuídas a essa instituição da UE.

[40] Entre 1999 e 2000, o Grupo de Trabalho do Art. 29.º emitiu cinco pareceres concernentes ao processo de negociações para a aprovação da Decisão "Porto Seguro" e ao nível de protecção assegurado pelo conjunto de princípios de "porto seguro". Todos estes pareceres podem ser consultados na página http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm (data da consulta: 05-01-2017).

Por força da decisão, foi permitido o livre fluxo de informações pessoais dos Estados-Membros da UE para empresas estabelecidas nos EUA quando estas subscreviam os princípios do "porto seguro" (art. 1.º, n.º 3). Se tal não acontecesse, a transferência não se operaria por não respeitar as normas europeias em termos da adequação do nível de protecção de dados, dadas as diferenças existentes entre os regimes dos dois lados do Atlântico. De referir que, embora a assinatura dos compromissos que constituem a Decisão "Porto Seguro" fosse voluntária, as regras aí consagradas eram vinculativas para todas as empresas que actuassem ao abrigo do mecanismo do "porto seguro".

Para aderir aos princípios de "porto seguro", a empresa americana deveria estipular na sua política de protecção da vida privada que deveria tornar pública a subscrição aos referidos princípios e sua efectiva concretização, bem como proceder à sua auto-certificação junto do Departamento do Comércio. Era esta instituição americana que ficava encarregue da análise de todas as auto-certificações e respectivas renovações anuais apresentadas pelas empresas, sendo ainda responsável pela supervisão do funcionamento do sistema "porto seguro" e supressão da lista de todas as empresas que não cumprissem os princípios.

À Comissão Federal do Comércio caberia, de acordo com o anexo V da decisão, tomar medidas coercivas em caso de violação, por parte das empresas americanas, dos compromissos assumidos no âmbito da Decisão "Porto Seguro". Tais medidas incluíam a realização de inquéritos sobre declarações falsas referentes à adesão aos princípios de "porto seguro" e sobre o não-acatamento destes princípios pelas empresas que actuavam no quadro da Decisão "Porto Seguro".

Nos termos desta decisão, as autoridades nacionais responsáveis pela protecção dos dados dos Estados-Membros tinham a capacidade de suspender as transferências de dados para as empresas certificadas, nomeadamente quando o Departamento do Comércio ou um mecanismo de recurso independente determinasse que a organização em causa não obedecia aos princípios de "porto seguro" ou quando existissem fortes indícios de que esses

princípios não estavam a ser observados (art. 3.º, n.º 1, alíneas *a)* e *b)*, da Decisão "Porto Seguro").

A Comissão podia proceder à adaptação ou suspensão da Decisão "Porto Seguro", assim como restringir o seu âmbito de aplicação, em qualquer momento e com base na experiência adquirida com a contínua vigência da Decisão. Em particular, tal podia suceder se as autoridades norte-americanas responsáveis pela observância dos princípios de "porto seguro" nos EUA não desempenhassem eficazmente as suas funções (art. 3.º, n.º 4) ou se o nível de protecção proporcionado pelos princípios de "porto seguro" tivesse sido ultrapassado por novos critérios da legislação norte-americana (art. 4.º, n. 1).

3.2. Importância

Se levarmos em conta que a transferência de dados pessoais da UE para os EUA envolve algumas das mais importantes e lucrativas empresas das sociedades modernas, e que esse fluxo de dados é essencial para a sua actividade, facilmente se compreendia a importância da Decisão "Porto Seguro" para a economia transatlântica.

O objectivo deste acordo era, portanto, o de possibilitar o funcionamento fluido do mercado sem que houvesse o receio, por parte das companhias norte-americanas, de que os cidadãos e as empresas europeias pudessem bloquear a transferência de dados pessoais ou intentar acções judiciais caso considerassem que as transferências punham em causa os seus direitos fundamentais.

3.3. Fragilidades

A vigência da Decisão "Porto Seguro" nunca foi pacífica, tendo surgindo, ao longo dos anos, diversas dúvidas sobre a sua substância e objectivos. Ainda antes de entrar em vigor, o Grupo de Trabalho do Art.º 29 manifestou preocupação relativamente a diversos aspectos da protecção de dados, que considerou não atingirem o nível pretendido. [41]

[41] GRUPO DE TRABALHO DO ART.º 29, "Parecer 4/2000 sobre o nível de protecção assegurado pelo conjunto de princípios de "Porto Seguro"", WP 32, Bruxelas, 16 de Maio de 2000.

A própria Comissão salientou algumas deficiências na Decisão "Porto Seguro" nas comunicações que adoptou. Na Comunicação de 27 de Novembro de 2013,[42] observou que as revelações sobre o programa PRISM da *National Security Agency* (NSA) norte-americana e a sua recolha ilegal de dados pessoais, com a ajuda de empresas certificadas no sistema "porto seguro", punham em causa a implementação da Decisão. De acordo com a Comissão, o PRISM possibilitava que os dados pessoais dos cidadãos europeus, enviados para os EUA no âmbito da Decisão "Porto Seguro", fossem acedidos e posteriormente tratados pelas autoridades norte-americanas de uma forma incompatível com os motivos pelos quais foram originalmente recolhidos na UE e com os fins para os quais foram transferidos para os EUA. Notou ainda que muitas empresas norte-americanas certificadas não respeitavam os princípios do "porto seguro", fragilizando a capacidade da Decisão "Porto Seguro" para garantir a segurança de dados pessoais e proteger os direitos fundamentais dos cidadãos da UE.

Tais críticas foram repetidas pela Comissão em outra Comunicação que adoptou a 27 de Novembro de 2013, onde referiu que as salvaguardas, em matéria de protecção de dados pessoais, fornecidas pela legislação norte-americana beneficiam sobretudos os cidadãos e os residentes legais dos EUA, não existindo qualquer possibilidade de *"os titulares de dados da UE ou dos EUA obterem acesso ou solicitarem a rectificação ou a supressão dos dados, ou apresentarem um recurso administrativo ou judicial caso, no âmbito de programas de vigilância dos EUA, os seus dados pessoais sejam recolhidos e tratados posteriormente".* [43]

As incertezas quanta à capacidade da Decisão "Porto Seguro" em harmonizar as regras sobre protecção de dados pessoais entre a UE e os EUA eram justificadas, em grande medida, pelo facto de o modelo europeu e o

[42] COMISSÃO EUROPEIA, "Comunicação da Comissão ao Parlamento Europeu e ao Conselho - Restabelecer a confiança nos fluxos de dados entre a UE e os EUA", COM(2013) 846 final, Bruxelas, 27 de Novembro de 2013.

[43] COMISSÃO EUROPEIA, "Comunicação da Comissão ao Parlamento Europeu e ao Conselho sobre o funcionamento do sistema «porto seguro» na perspectiva dos cidadãos da UE e das empresas estabelecidas na UE", COM(2013) 847 final, 27 de Novembro de 2013. P. 19.

norte-americano abordarem de maneira diferente a questão da protecção de dados pessoais.

Na UE, procurou-se estruturar o seu regime em torno da defesa dos direitos fundamentais e assentá-lo em uma estrutura jurídica uniforme que vigore em todo o espaço europeu. De modo a garantir que os direitos dos cidadãos europeus são efectivamente respeitados, exige-se a criação de agências governamentais independentes para a protecção de dados pessoais e, em alguns casos, o consentimento prévio dos titulares para o tratamento dos seus dados.[44]

Fundamentalmente distinto, o modelo vigente nos EUA caracteriza-se pelo foco na promoção dos fluxos de dados e pelo seu carácter fragmentado, existindo uma multiplicidade de instrumentos jurídicos que só se aplicam em determinados sectores, tipos de dados ou Estados.

Tal deveu-se ao facto de a Quarta Emenda da Constituição dos EUA, que tutela a privacidade e que passou a abranger também os dados pessoais a partir de 1967 com o caso *Katz vs. United States*[45]*,* já não ser suficiente para proteger o direito à privacidade dos riscos criados pelas novas tecnologias. Por esta razão, muitas das leis relacionadas com a protecção de dados foram criadas precisamente com o objectivo de preencher lacunas legislativas que ameaçavam o direito à privacidade, como, por exemplo, o *The Fair Credit Reporting Act* [46] ou o *Electronic Communications Privacy Act.*[47]

---

[44] DEPARTAMENTO DO COMÉRCIO DOS ESTADOS UNIDOS, "U.S.-EU Safe Harbor Overview", 18 de Dezembro de 2013 (última actualização). Disponível em https://build.export.gov/main/%20safeharbor/eu/eg_main_018476 (data da consulta: 05-01-2017).

[45] Nesta decisão do Supremo Tribunal de Justiça dos Estados Unidos, foi entendida que a protecção consagrada na Quarta Emenda da Constituição Norte-Americana aplica-se em qualquer situação em que o indivíduo tenha uma expectativa objectivamente razoável de privacidade, assim como foi decidido que a noção de "buscas e apreensões não razoáveis" envolve as escutas telefónicas, já que estas podem violar o direito à privacidade do indivíduo.

[46] Promulgado em 1970 pelo Congresso dos Estados Unidos, destina-se a promover a precisão imparcialidade e privacidade das informações sobre o consumidor que estejam em arquivos das empresas de informação ao consumidor, regulando, para isso, a forma como a informação pode ser recolhida, partilhada e utilizada. Juntamente com o *Fair Debt Collection Practices Act,* constitui a fundação da lei dos consumidores nos Estados Unidos.

[47] Aprovado pelo Congresso dos Estados Unidos em 1986, visava, entre outros objectivos, alargar as restrições governamentais às escutas telefónicas de forma a aplicarem-se também às transmissões de dados electrónicos. Considerado desactualizado, foi alterado pelo

Em resultado da inexistência de uma legislação federal única sobre a protecção de dados, incentiva-se a auto-regulação das empresas e a resolução do caso em concreto de acordo com as suas especificidades. [48] Embora a auto-regulação possa beneficiar as empresas devido à flexibilidade na aplicação da lei, tem a desvantagem de criar incertezas quanto às limitações e responsabilidades das empresas no tratamento de dados pessoais e aos direitos dos titulares dos dados.

Em virtude disso, a própria Comissão Federal do Comércio, em Março de 2012, reconheceu as insuficiências da auto-regulação e sugeriu ao Congresso dos EUA a aprovação de uma legislação única em matéria de protecção de dados, com vista a alcançar uma maior adequação do nível de protecção de dados pessoais assegurado pelo país.[49]

Não obstante as fraquezas apontadas à protecção de dados pessoais nos EUA e o reconhecimento da necessidade de introduzir modificações na Decisão "Porto Seguro", a Comissão considerou que a sua revogação iria afectar gravemente os interesses das empresas europeias e americanas que fossem membros do sistema, pelo que seria preferível que este continuasse em vigor. [50]

Communications Assistance for Law Enforcement Act em 1994, *USA Patriot Act* em 2001, leis de reautorização do *USA Patriot Act* em 2006 e *FISA Amendments Act* em 2008.

[48] DONEDA, Danilo, *Da privacidade à protecção de dados pessoais,* Renovar, 2006. P. 305 e pp. 317-320.

[49] COMISSÃO FEDERAL DO COMÉRCIO, "Protecting Consumer Privacy in an Era of Rapid Change: Recommendation For Businesses and Policymakers", Março de 2012. Pp. 11 – 14. Disponível em https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf (data da consulta: 05-01-2017).

[50] COMISSÃO EUROPEIA, "Comunicação da Comissão ao Parlamento Europeu e ao Conselho - Restabelecer a confiança nos fluxos de dados entre a UE e os EUA", COM(2013) 846 final, Bruxelas, 27 de Novembro de 2011. P. 8.

4. A DECISÃO "PORTO SEGURO" NO TRIBUNAL DE JUSTIÇA

4.1. Enquadramento Factual

O Acórdão Schrems veio impedir que a Decisão "Porto Seguro" sirva de base legal para a maioria das transferências de dados pessoais da UE para os EUA, ao declará-la inválida por não oferecer garantias de protecção dos dados pessoais e garantias de meios em caso de lesão dos dados pessoais.

Maximillian Schrems tornou-se conhecido por ter fundado, em 2011, a organização não-governamental *Europe versus Facebook*, que se dedica a divulgar e a contestar as práticas mais controversas, em matéria de protecção de dados pessoais e de respeito pela privacidade dos seus utilizadores, da maior rede social a nível internacional, com cerca de 1.590 milhões de usuários activos e 18% de quota de mercado: o *Facebook*.[51]

O grupo surgiu quando, no decurso de uma investigação para um trabalho académico, Schrems descobriu que o *Facebook* armazena e utiliza os dados pessoais dos seus utilizadores, inclusive informações que estes pensavam ter eliminado. Posteriormente, e após tomar conhecimento que a empresa possibilitava aos cidadãos europeus o exercício do direito de acesso às informações que lhes digam respeito e que estejam na posse do *Facebook*, tal como era imposto pela Decisão "Porto Seguro"[52], Schrems avançou com um pedido à empresa norte-americana, para que esta lhe enviasse uma cópia de todos os dados que possuísse sobre si. [53]

Em resposta, foram-lhe entregues, em formato de CD, mais de 1.200 páginas, com a descrição detalhada de todos os seus movimentos no *Facebook* desde da sua adesão em 2008. Entre as informações recolhidas ao longo dos anos, constavam todas as amizades feitas e desfeitas, todos os eventos a que tinha sido convidado e as respostas que deu, os endereços de

[51] CHAFREY, Dave, "Global social media research summary 2016", *Smart Insights,* 8 de Agosto de 2016. Disponível em http://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research/ (data da consulta: 05-01-2017).
[52] Anexo I da Decisão "Porto Seguro" – Princípios de «Porto Seguro» (Protecção da Vida Privada), *Jornal Oficial das Comunidades Europeias*, 25 de Agosto de 2000, p. 12.
[53] De modo a solicitar uma cópia dos dados que estejam na posse do Facebook, Schrems teve que enviar um comprovativo de identidade, um endereço de *e-mail*, a morada e o *link* para a sua página de perfil.

e-mails de contactos dos seus amigos que não tinham sido obtidos por si e todas as conversas e mensagens, inclusive as que tinha apagado.

Uma vez que é na Irlanda que está localizada a filial europeia do *Facebook*, Schrems decidiu denunciar a situação ao *Data Protection Commissioner* irlandês (Comissário irlandês para a Protecção de Dados), acusando a empresa norte-americana de reter os dados que os seus utilizadores tinham eliminado e de não lhe ter enviado todas as informações que detém sobre ele. De modo a captar a atenção dos principais meios de comunicação social e do público em geral para o seu caso, editou as informações pessoais que o *Facebook* lhe tinha entregado e publicou-as na página *online* do *Europe versus Facebook* [54]*,* o que motivou vários utilizadores dessa rede social a solicitarem igualmente ao *Facebook* o envio dos seus dados.

Relativamente à acusação de não ter entregue a totalidade das informações pessoais em seu poder, o *Facebook* justificou-se com o argumento de que alguns dos dados em falta fazem parte da sua propriedade industrial e constituem segredo comercial, isto é, são informações cuja divulgação é interdita por comprometer seriamente a actividade da empresa, devido ao valor comercial que as mesmas representam para esta. [55]

Schrems apresentou vinte e três queixas ao Comissário irlandês para a Protecção de Dados (doravante, "Comissário") em que questionava a política de privacidade do *Facebook Inc*. Por não serem financeiramente viáveis e pela morosidade em obter uma decisão do Comissário, o activista austríaco optou por desistir de vinte e duas das queixas que tinha formulado.[56]

Na única que manteve, Schrems alegava que a Agência de Segurança Nacional norte-americana (*National Security Agency* (NSA)) tinha acesso

[54] EUROPE VERSUS FACEBOOK, "Facebook's Data Pool". Disponível em http://europe-v-facebook.org/EN/Data_Pool/data_pool.html (data da consulta: 05-01-2017).
[55] PROTALINSKI, Emil, "Facebook: Releasing your personal data reveals our trade secrets", *ZD Net,* 12 de Outubro de 2011. Disponível em http://www.zdnet.com/article/facebook-releasing-your-personal-data-reveals-our-trade-secrets/ (data da consulta: 05-01-2017).
[56] EUROPE VERSUS FACEBOOK, "Legal Procedure against "Facebook Ireland Limited". Disponível em http://europe-v-facebook.org/EN/Complaints/complaints.html (data da consulta: 05-01-2017).

generalizado aos dados pessoais dos cidadãos europeus que estavam na posse do *Facebook Inc*, após terem sido transferidos pelo *Facebook Ireland*, no âmbito de um programa designado "PRISM", onde o acesso em massa a esses dados, por razões de espionagem, segurança nacional e outros assuntos e sem que houvesse um motivo plausível, era consentido.[57] Será precisamente essa queixa que deu origem ao Acórdão Schrems.

A 25 de Junho de 2013, Schrems apresentou queixa junto do Comissário irlandês para a Protecção de Dados para que este, exercendo as suas competências estatuárias, proibisse a filial *Facebook Ireland* de transferir os seus dados pessoais para a sede, *Facebook Inc.*, situada em território norte-americano, onde seriam alvo de tratamento. No texto, alegava que o direito e as práticas em vigor nos EUA não asseguravam uma protecção adequada dos dados pessoais contra as actividades de vigilância aí praticadas pelas autoridades públicas, mencionando as revelações feitas por Edward Snowden[58] sobre as actividades dos serviços de informação norte-americanos, nomeadamente as da Agência de Segurança Nacional. [59]

Por entender que não lhe competia investigar os factos denunciados, o Comissário arquivou a queixa por falta de fundamento, uma vez que considerava não existir provas de que a Agência de Segurança Nacional tivesse tido acesso aos dados pessoais de Schrems. Acrescentou ainda que as críticas feitas ao nível de protecção dos dados pessoais nos EUA tinham que ser decididas em conformidade com a Decisão "Porto Seguro", na qual a

[57] SCHREMS, Maximilian, "Complaint against Facebook Ireland Ltd – 23 "PRISM"", Viena, 25 de Junho de 2013. Disponível em http://www.europe-v-facebook.org/prism/facebook.pdf (data da consulta: 05-01-2017).

[58] Edward Snowden tornou-se mundialmente célebre após divulgar para a imprensa documentos secretos sobre as práticas de vigilância em massa cometidas pela Agência de Segurança Nacional (NSA) norte-americana, da qual era colaborador, em 2013. Tais documentos atestavam a existência do PRISM, um sistema de vigilância cujo objectivo é o de, em tempo real, vigiar e monitorizar toda a actividade das telecomunicações através da recolha de dados pessoais fornecidos por empresas multinacionais como a *Microsoft* e o *Facebook*. Acusado pelas autoridades norte-americanas de espionagem, roubo e divulgação de documentos confidenciais que estavam na posse do Governo dos EUA, Snowden encontra-se a viver na Rússia, onde lhe foi concedido asilo político, tendo sido já lançadas várias petições para que seja concedido um perdão a Snowden.

[59] Acórdão Schrems §28.

Comissão considerou como adequado o nível de protecção oferecido nos EUA, pelo que não podiam ser invocadas. [60]

Por conseguinte, Schrems interpôs recurso da decisão em causa para o *High Court* (Supremo Tribunal de Justiça) irlandês, que, após analisar as provas, declarou que a intercepção de dados pessoais transferidos da UE para os EUA correspondiam a finalidades necessárias e indispensáveis ao interesse público. Todavia, admitiu que os cidadãos da UE não dispõem de nenhum direito efectivo a serem ouvidos, dada a supervisão das acções dos serviços de informações ser feita através de procedimentos secretos e não contraditórios, impedindo os cidadãos europeus de contestarem os "excessos consideráveis" cometidos pela Agência de Segurança Nacional e outros órgãos americanos em matéria de acesso e uso dos seus dados pessoais. [61]

Nesse sentido, o *High Court* observou que a Constituição irlandesa qualifica como contrário ao princípio da proporcionalidade e aos direitos e liberdades fundamentais o acesso massivo e indiscriminado a dados pessoais. Para que as intercepções das comunicações electrónicas estejam conformes ao texto fundamental irlandês é preciso provar o seu carácter selectivo, que a vigilância da pessoa ou grupo em causa se justifica com interesses de defesa nacional ou de combate à criminalidade e a existência de garantias adequadas e verificáveis.

Logo, de acordo com o *High Court*, caso o processo fosse julgado somente com base no direito irlandês, e visto existir uma dúvida séria sobre se os EUA asseguram um nível adequado de protecção de dados pessoais, o Comissário devia ter iniciado uma investigação aos factos denunciados na queixa, não havendo motivo para arquivá-la. [62]

O *High Court* considerou, contudo, que as questões suscitadas na queixa devem ser apreciadas à luz do direito da UE, designadamente dos arts. 7.º, 8.º e 47.º da Carta e dos arts. 25.º, n.º 6, e 28.º da Directiva, tendo em

[60] Acórdão Schrems §29.
[61] Acórdão Schrems §31.
[62] Acórdão Schrems §33.

conta a decisão do TJUE no Acórdão *Digital Rights Ireland*. Em causa estaria, portanto a validade da Decisão "Porto Seguro".[63]

O *High Court* decidiu, então, suspender a instância e reenviar as questões prejudiciais seguintes para o TJUE: a primeira, se o Comissário está vinculado em termos absolutos à orientação estabelecida na Decisão "Porto Seguro"; a segunda, se pode proceder à sua própria investigação sobre o assunto, dados os desenvolvimentos recentes ocorridos desde a entrada em vigor da decisão da Comissão.[64]

4.2. A Decisão

4.2.1. Os Poderes das Autoridades Nacionais de Controlo perante uma Decisão da Comissão

O TJUE veio examinar as questões prejudiciais colocadas pelo *High Court* em acórdão de 6 de Outubro de 2015, começando por abordar a referente à clarificação dos poderes das autoridades nacionais de controlo, na acepção do art. 28.º da Directiva 95/46, perante uma decisão da Comissão adoptada de acordo com os termos do art. 25.º, n.º 6 dessa directiva.

A esse respeito, começa por recordar que a UE impõe, através do art. 28.º, n.º1, da Directiva, que todos os Estados-Membros instituam uma ou mais autoridades públicas incumbidas de fiscalizar, de forma independente, o cumprimento das regras europeias relativas à protecção de pessoas singulares no que concerne ao tratamento dos seus dados pessoais efectuados no território do Estado-Membro a que pertençam. [65]

Neste contexto, refere que a transferência de dados de um Estado-Membro para um país terceiro é definida como tratamento de dados pessoais no art. 2.º, al. b), da Directiva, visto nesta indicar-se, a título de exemplo, a

[63] Acórdão Schrems §34.
[64] Conclusões do advogado-geral Yves Bot, apresentadas em 23 de Setembro de 2015, no Processo C-362/14 – *Maximillian Schrems contra Data Protection Comissioner* [pedido de decisão prejudicial apresentado pelo High Court (Irlanda)], §47. Disponível em http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A62014CC0362 (data da consulta: 05-01-2017).
[65] Acórdão Schrems §41.

"comunicação por transmissão, difusão ou qualquer outra forma de colocação à disposição" como uma forma de operação efectuada sobre dados pessoais. [66]

Quando há uma decisão da Comissão que reconheça como adequado o nível de protecção de dados pessoais num país terceiro, como é o caso da Decisão "Porto Seguro", os Estados-Membros e os seus órgãos estão impedidos de tomar medidas contrárias a essa decisão, dado esta gozar de uma presunção de legalidade que se manterá enquanto não for declarada inválida pelo Tribunal de Justiça.

Contudo, tal não deve impossibilitar aos cidadãos europeus de apresentarem, junto das autoridades nacionais de controlo, um pedido para a protecção dos seus direitos e liberdades no que diz respeito à transferência dos seus dados pessoais num país terceiro e ao tratamento dos mesmos aí efectuado, nos termos do art. 28.º, nº 4, da Directiva. [67] Caso contrário, estar-se-ia a atribuir a uma decisão dessa natureza a capacidade de suprimir ou reduzir os poderes de investigação expressamente reconhecidos às autoridades nacionais de controlo no artigo 8.º, n.º 3, da Carta e no art. 28.º da mencionada directiva. [68]

Além disso, o exercício do direito, assegurado pelo art. 8.º, n.º 1 e n.º 3 da Carta, de poder apresentar pedidos às autoridades nacionais de controlo para efeitos de protecção dos seus direitos fundamentais estaria interdito àqueles cujos dados pessoais tivessem sido ou pudessem ser transferidos para o país terceiro em causa, o que seria contrário às finalidades de defesa dos direitos e liberdades estabelecidas pela Directiva.[69]

Atendendo a estas considerações, o TJUE declarou que, perante um pedido referente à protecção dos direitos e liberdades do queixoso no que respeita à transferência dos seus dados pessoais para um país terceiro, feita ao abrigo de uma decisão da Comissão, e onde põe em causa, como no caso em apreço, a compatibilidade da Decisão "Porto Seguro" com a protecção das

[66] Acórdão Schrems §45.
[67] Acórdão Schrems §52 e 53.
[68] Acórdão Schrems §56.
[69] Acórdão Schrems §58 e 59.

liberdades e direitos fundamentais das pessoas, cabe à autoridade responsável examiná-la e decidi-la com toda a diligência necessária. [70]

Neste caso, se a referida autoridade concluir que os elementos em que assenta esse pedido são infundados, deve arquivá-la, devendo o queixoso ter acesso às vias de recurso jurisdicionais que lhe permitam impugnar essa decisão junto dos órgãos jurisdicionais nacionais, que, caso considerem os fundamentos apresentados procedentes, deverão suspender o processo e apresentar ao TJUE um pedido de decisão prejudicial de apreciação da validade. [71]

Na situação oposta, ou seja, se entender que a queixa tem fundamento e que a Decisão "Porto Seguro" não garante um nível de protecção adequado, a autoridade referida deve invocar, pelas vias de recurso previstas na legislação nacional, as críticas que considere válidas perante os tribunais nacionais para que estes, caso partilhem das mesmas dúvidas quanto à validade da decisão da Comissão, suscitem um reenvio prejudicial para que a validade dessa decisão seja apreciada pelo TJUE.[72]

Em suma, ainda que exista uma decisão da Comissão, tomada nos termos do art. 25.º, n.º 6, da Directiva, que qualifique como adequado o nível de protecção de dados pessoais oferecido por um país terceiro, nada obsta a que as autoridades nacionais de protecção de dados, no seguimento de uma queixa que conteste o sentido dessa decisão, utilizem os seus poderes de investigação para averiguar a procedência dos factos alegados no pedido.

4.2.2. Validade da Decisão "Porto Seguro"

Resolvida a primeira questão, o TJUE prosseguiu para a avaliação da validade da Decisão "Porto Seguro", procurando responder às alegações, expressas por Schrems na sua queixa, de que essa decisão não está conforme às exigências que decorrem da Directiva, dado o direito e as práticas norte-americanas não assegurarem um nível de protecção adequado.

[70] Acórdão Schrems §63.
[71] Acórdão Schrems §64.
[72] Acórdão Schrems §65.

Para isso, começa por estabelecer o enquadramento jurídico no qual irá assentar a sua avaliação. Embora não seja dada na Directiva nenhuma definição do conceito de nível de protecção adequado, entende-se que constatamos a sua existência quando o país terceiro, por força da sua legislação interna ou dos seus compromissos internacionais, garanta, de modo efectivo, um nível de protecção do direito à vida privada e das liberdades e direitos fundamentais das pessoas substancialmente equivalente ao conferido dentro da UE, como resulta do art. 25.º, n.º 6, da Directiva.[73]

Com a exigência de um nível de protecção adequado ao país terceiro para o qual os dados pessoais são transferidos, não se pretende dizer que o país em causa tenha que assegurar um nível idêntico ao garantido no espaço europeu: exige-se, isso sim, que os meios judiciais usados por esse país sejam eficazes a assegurarem uma protecção substancialmente equivalente à garantida dentro da UE, independentemente de serem ou não diferentes dos meios desenvolvidos pela UE para o cumprimento dos requisitos decorrentes da Directiva. [74]

Assim, quando encarregue de analisar o nível de protecção vigente num país terceiro, à Comissão é exigido que aprecie o conteúdo das regras aplicadas nesse país, resultantes da legislação interna ou de compromissos internacionais, assim como a prática destinada a asseverar o cumprimento de tais regras, devendo ainda ter em atenção as circunstâncias que digam respeito a uma transferência de dados para um país terceiro.

Dada a possibilidade de o nível de protecção vir a sofrer modificações com a evolução dos tempos, a Comissão está igualmente encarregue de, após a adopção de uma decisão de adequação, averiguar periodicamente se a constatação atinente ao nível de protecção oferecido pelo país terceiro em causa mantém-se justificada pela realidade e pelo direito. A este ponto, acrescenta-se que essa verificação impõe-se quando surjam indícios que suscitem incertezas a esse respeito. [75]

[73] Acórdão Schrems §73.
[74] Acórdão Schrems §74.
[75] Acórdão Schrems §76.

Além disso, segundo o TJUE, as circunstâncias que ocorram posteriormente à adopção de uma decisão da Comissão nos termos do art. 25.º, n.º 6, da Directiva devem ser tidas em conta quando esteja em análise a validade dessa decisão. [76]

Todos estes elementos levam o TJUE a concluir que, visto que o poder de apreciação da Comissão quanto à adequação do nível de protecção assegurado por um país terceiro ser reduzido, deve-se, então, proceder a uma fiscalização estrita das exigências decorrentes do art. 25.º da Directiva, lido à luz da Carta.

No que diz respeito à Decisão "Porto Seguro", qualifica o sistema aí consagrado como sendo de auto-regulação. Devido a essa particularidade, considera ser necessário o desenvolvimento de mecanismos de detenção e de fiscalização que assegurem a clara identificação e punição de qualquer violação das normas destinadas à protecção dos direitos fundamentais, de forma a garantir o funcionamento de tal sistema. [77]

É constatado pelo TJUE que os princípios de "porto seguro" são apenas aplicáveis às empresas norte-americanas auto certificadas que recebam dados pessoais da UE, não estando as autoridades públicas americanas sujeitas ao cumprimento desses princípios.[78] Observa ainda que, nessa decisão, não se encontram referências suficientes à forma como os EUA garantem um nível de protecção adequado, por força da sua legislação interna ou dos seus compromissos internacionais.[79]

Estes aspectos ganham particular importância quando se verifica que o quarto parágrafo do anexo I da Decisão "Porto Seguro" consagra a possibilidade de restringir a aplicabilidade dos princípios mencionados por questões de segurança nacional, interesse público ou execução da lei, assim

[76] Acórdão Schrems §77.
[77] Acórdão Schrems §81.
[78] Acórdão Schrems §82.
[79] Acórdão Schrems §83.

como de cumprimento de obrigações contraditórias provenientes de legislação, regulamento governamental ou jurisprudência.[80]

Portanto, quando constem na legislação norte-americana requisitos de segurança nacional, interesse público ou execução da lei que sejam incompatíveis com a aplicação dos princípios de "porto seguro", as organizações norte-americanas auto certificadas que recebam dados pessoais da UE estão obrigadas a favorecer a aplicação das regras internas, afastando-se dos princípios conflituantes que constem na Decisão "Porto Seguro".[81]

Por força da consagração do primado desses requisitos sobre os princípios de "porto seguro", gera-se a possibilidade de eventuais ingerências, fundadas nesses requisitos, nos direitos fundamentais dos cidadãos europeus cujos dados tenham sido ou possam ser transferidos para os EUA. No entanto, a Decisão "Porto Seguro" não faz referência a normas norte-americanas de carácter estatal que regulem e limitem essas ingerências, bem como a mecanismos eficazes de protecção legal que estejam disponíveis aos particulares para contestarem esse tipo de interferências. [82]

Devido à ausência de um critério que delimite o acesso das autoridades estatais aos dados e a sua utilização posterior para fins precisos, estritamente necessários e susceptíveis de legitimar essa ingerência, as autoridades norte-americanas podem aceder aos dados pessoais provenientes da UE e dar-lhes um tratamento distinto daquele que justificou a sua transferência. [83]

Em resultado disso, o TJUE afirma que a Decisão "Porto Seguro" não dispõe de garantias que permitam proteger eficazmente os dados transferidos contra os riscos de abuso e contra qualquer acesso e utilização ilícita, facultando lesões aos direitos fundamentais de respeito pela vida privada e de protecção de dados pessoais, consagrados nos arts. 7.º e 8.º da Carta.

Do mesmo modo, observa que a falta de previsão na Decisão "Porto Seguro" de vias de direito administrativas ou judiciais a que os particulares

[80] Acórdão Schrems §84 e 85.
[81] Acórdão Schrems §86.
[82] Acórdão Schrems §87 e 88.
[83] Acórdão Schrems §90.

possam recorrer quando queiram aceder aos dados pessoas que lhe dizem respeito, ou a possibilidade de os rectificar ou de suprimi-los, constitui uma violação da essência do direito fundamental a uma protecção jurisdicional efectiva, previsto no art. 47.º da Carta. [84]

Em consequência das razões apresentadas, o TJUE decidiu declarar como inválido o art. 1.º da Decisão "Porto Seguro" por não cumprir a exigência de constatar que os EUA garantem efectivamente um nível de protecção adequado, por força da sua legislação interna ou dos seus compromissos internacionais, nos termos do art. 25.º, n.º 6, da Directiva. De referir ainda que, por entender não ser necessário, o TJUE prescindiu expressamente de examinar o conteúdo dos princípios de "porto seguro". [85]

Foram igualmente tecidas críticas ao art. 3.º, n.º 1, da Decisão "Porto Seguro". Nessa norma, estabelece-se que as autoridades nacionais de controlo dispõem de competência para tomar as medidas necessárias para garantir o cumprimento das disposições nacionais adoptadas em execução da Directiva, afastando, no entanto, a hipótese de essas autoridades poderem adoptar medidas destinadas a garantir o respeito pelo art. 25.º da Directiva. [86]

Tal disposição traduz-se, no entender do TJUE, numa limitação dos poderes que são conferidos às autoridades nacionais quando lhes seja apresentado um pedido susceptível de pôr em causa uma decisão da Comissão que tenha avaliado como adequado o nível de protecção de dados pessoais assegurado por um país terceiro. [87]

Ao restringir deste modo os poderes das autoridades nacionais de controlo, a Comissão actuou num sentido que vai para além da competência que lhe é conferida pelo art. 25.º, n.º 6, da Directiva, razão pela qual o TJUE decidiu declarar a invalidade do art. 3.º, n.º 1, da Decisão "Porto Seguro". [88]

Em consequência das apreciações feitas no acórdão, juntamente com o facto de ter considerado os arts. 2.º e 4.º inválidos por serem indissociáveis

[84] Acórdão Schrems §94.
[85] Acórdão Schrems §98.
[86] Acórdão Schrems §101.
[87] Acórdão Schrems §102.
[88] Acórdão Schrems §103 e 104.

daqueles que analisou anteriormente, o TJUE optou por considerar globalmente inválida a Decisão "Porto Seguro".[89]

4.2.3. Síntese Conclusiva

No decorrer da sua sentença de 6 de Outubro de 2015, o TJUE observa que a decisão de adequação da Comissão é parca no que diz respeito a indicações do modo como os EUA asseguram um nível de protecção de dados pessoais considerado equivalente àquele que vigora na UE.

Além disso, ao estar consagrada a hipótese de as autoridades norte-americanas restringirem a aplicabilidade dos princípios de "Porto Seguro", por razões de segurança nacional, interesse público ou execução ou para darem prioridade ao cumprimento de obrigações contraditórias provenientes do direito interno, cria-se a possibilidade de existirem ingerências nos direitos fundamentais dos titulares dos dados transferidos sem que essas estejam devidamente reguladas no direito norte-americano.

Por força desses factores, as autoridades norte-americanas poderão aceder aos dados pessoais provenientes da UE e dar-lhes um tratamento que seja desconforme com os princípios de "Porto Seguro" e com as regras europeias em matéria de protecção de dados e de respeito pela vida privada, uma vez que a Decisão "Porto Seguro" não dispõe de um critério objectivo que restrinja o acesso das autoridades estatais aos dados e a sua utilização posterior ao estritamente necessário para o alcance de fins específicos.

Essa falha da decisão da Comissão torna-se mais grave quando se nota a ausência de vias de direito administrativas ou judiciais a que os cidadãos europeus possam recorrer quando pretendam contestar o acesso ilegítimo das autoridades norte-americanas aos seus dados pessoais. O conteúdo essencial do direito fundamental a uma tutela jurisdicional efectiva é, desta forma, infringido.

A restrição dos poderes das autoridades nacionais de controlo quando lhes seja entregue um pedido que coloque em causa a apreciação, feita na Decisão "Porto Seguro", do nível de protecção de dados pessoais assegurado

[89] Acórdão Schrems §105 e 106.

pelos EUA é igualmente problemática, uma vez que cabe às autoridades nacionais de controlo examinarem, com toda a independência, se as transferências realizadas ao abrigo dessa decisão da Comissão obedecem às exigências impostas pela Directiva.

Ao adoptar a Decisão "Porto Seguro", a Comissão não podia reduzir os poderes de que dispõem as autoridades nacionais de controlo, uma vez que estas têm o dever de dar resposta a qualquer pedido em que o seu autor solicite a protecção dos seus direitos e liberdades ou a verificação da licitude de qualquer tratamento de dados.

É de realçar que argumentos semelhantes aos que foram referidos pelo TJUE para a defesa da tese da invalidade da Decisão "Porto Seguro" já tinham sido alegados anteriormente por outros órgãos europeias, nomeadamente em um parecer do Grupo de Trabalho do Art. 29.º [90] e em duas comunicações da Comissão.[91]

De certo modo, pode-se dizer que, ao declarar a invalidade da Decisão "Porto Seguro", o TJUE limitou-se a pôr fim à vigência de um acordo cujas fragilidades na protecção dos dados pessoais dos cidadãos europeus eram já amplamente reconhecidas.

Assim, pelos motivos expostos, concorda-se com as razões que levaram o TJUE a decidir pela declaração de invalidade da Decisão "Porto Seguro" no Acórdão Schrems.

4.3. Consequências

Ao declarar a ilegalidade da Decisão "Porto Seguro", o acórdão do TJUE teve um impacto que ultrapassa a esfera do processo em que se insere: alterou a base legal que fundamentava a transferência dos dados pessoais dos

[90] GRUPO DE TRABALHO DO ART. 29.º, "Parecer 4/2000 sobre o nível de protecção assegurado pelo conjunto de princípios de "Porto Seguro"", WP 32, Bruxelas, 16 de Maio de 2000.

[91] COMISSÃO EUROPEIA, "Comunicação da Comissão ao Parlamento Europeu e ao Conselho - Restabelecer a confiança nos fluxos de dados entre a UE e os EUA", COM(2013) 846 final, Bruxelas, 27 de Novembro de 2013, e "Comunicação da Comissão ao Parlamento Europeu e ao Conselho sobre o funcionamento do sistema «porto seguro» na perspectiva dos cidadãos da UE e das empresas estabelecidas na UE", COM(2013) 847 final, 27 de Novembro de 2011.

cidadãos europeus para os EUA, bem como o enquadramento no qual assentava a defesa dos particulares e empresas europeias perante uma transferência dos seus dados para território norte-americano que fosse lesiva dos seus direitos.

Mesmo que haja outros meios legais que assegurem a adequação do nível de protecção conferido pelos EUA aos dados pessoais transferidos, o certo é que a decisão do TJUE cria uma lacuna na regulação das relações comerciais transatlânticas que, dada a crescente importância da transferência de dados pessoais para o comércio internacional, necessita de ser resolvida. Na sequência do acórdão, a Comissão Nacional de Protecção de Dados, à semelhança do que fizeram as autoridades de protecção de dados de outros Estados-Membros, deliberou a suspensão da migração dos dados pessoais dos cidadãos portugueses para os EUA até então feitas ao abrigo da Decisão "Porto Seguro".[92]

4.3.1. Bases Alternativas para as Transferências Transatlânticas

Para contribuir para o esclarecimento sobre as condições em que as transferências transatlânticas de dados pessoais podem continuar a operar, o Grupo de Trabalho do art. 29.º, que reúne as 28 autoridades nacionais de protecção de dados, bem como a AEPD, emitiu, a 16 de Outubro de 2015, uma declaração sobre as conclusões que se deve retirar do acórdão em estudo.[93] Nela, começa por apelar aos Estados-Membros e às instituições que dialoguem com as autoridades norte-americanas de forma a encontrarem novas soluções técnicas e jurídicas para as transferências de dados, sugerindo como possível parte da solução as negociações para um novo acordo "Porto Seguro".

[92] COMISSÃO NACIONAL DE PROTECÇÃO DE DADOS, "Transferências de dados pessoais para os EUA: CNPD emite autorizações provisórias até conclusão do estudo sobre impacto do acórdão do Tribunal de Justiça da EU", 23 de Outubro de 2015. Disponível em https://www.cnpd.pt/bin/relacoes/comunicados/Comunicado_CNPD_SafeHarbor.pdf (data da consulta: 05-01-2017).

[93] GRUPO DE TRABALHO DO ART. 29.º, "Statement on the implementation of the judgement of the Court of Justice of the European Union of 6 October 2015 in the Maximilian Schrems v Data Protection Commissioner case (C-362-14)", Bruxelas, 16 de Outubro de 2015. Disponível em http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf (data da consulta: 05-01-2017).

Quanto aos instrumentos jurídicos alternativos a empregar nas transferências de dados, uma vez que os previstos na Decisão "Porto Seguro" já não podem ser mais utilizados, o Grupo de Trabalho do art. 29.º indica como possíveis as cláusulas contratuais-tipo de protecção de dados e as regras vinculativas para empresas, ou, como são designadas na declaração, as *binding corporate rules* (BCR), embora o impacto do acórdão sobre estes instrumentos ainda careça de ser estudado pelo Grupo de Trabalho do art. 29.º.

Na sua declaração, o Grupo de Trabalho do art. 29.º anuncia igualmente que as autoridades de protecção de dados adoptarão todas as medidas necessárias e apropriadas, no caso de não ser acordada nenhuma solução com as autoridades norte-americanas.

Por último, realça a responsabilidade partilhada das autoridades de protecção de dados, das instituições da UE, dos Estados-Membros e das empresas para obterem soluções sustentáveis que dêem execução às constatações feitas pelo TJUE no acórdão. Particularmente, exorta as empresas a ponderarem a introdução de mecanismos técnicos e jurídicos para mitigar eventuais riscos que possam ocorrer aquando a transferência de dados.

Os instrumentos jurídicos alternativos aos quais as empresas podem recorrer até que seja alcançado um novo acordo transatlântico foram analisados com mais detalhe na comunicação que a Comissão emitiu a 6 de Novembro de 2015.[94] Após examinar as vantagens e desvantagens de cada um dos instrumentos disponíveis, reiterou a necessidade da elaboração de um novo quadro para a transferência de dados pessoais para os EUA.

Essa é, no entender da Comissão, a solução que melhor assegura a continuidade da protecção dada aos dados pessoais dos cidadãos europeus quando são transferidos para os EUA e a mais favorável para o comércio transatlântico, visto proporcionar um mecanismo de transferência menos

[94] COMISSÃO EUROPEIA, "Comunicação da Comissão ao Parlamento Europeu e ao Concelho sobre a transferência de dados pessoais da UE para os Estados Unidos da América ao abrigo da Diretiva 95/46/CE na sequência do acórdão proferido pelo Tribunal de Justiça no processo C-362/14 (Schrems)", COM(2015) 566 final, Bruxelas, 6 de Novembro de 2015. Disponível em http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52015DC0566 (data da consulta: 05-01-2017).

complexo e dispendioso, agora que a Decisão "Porto Seguro" foi declarada inválida. Não obstante o sua utilização ser legítima, as bases alternativas para as transferências de dados pessoais têm a desvantagem de responsabilizar os exportadores de dados da protecção assegurada pelo país terceiro aos dados pessoais transferidos e, no caso das derrogações previstas no artigo 26.º, n.º 1, da Directiva, de não serem adequadas para as transferências de dados que sejam frequentes, volumosas e estruturais.

4.3.2. Novos Critérios de Aplicação do Art. 25.º, n.º 2 e n.º 6, da Directiva 95/46/CE.

A decisão do TJUE em apreço estabeleceu ainda novos critérios de apreciação do nível de protecção conferido pelo país terceiro aos dados pessoais, que deverão ser seguidos pela Comissão quando adoptar uma decisão nos termos do art. 25.º, n.º 2 e n.º 6, da Directiva. Esses novos requisitos são, aliás, semelhantes àqueles que estão previstos no art. 41.º, n.º 2, da proposta de Regulamento (art. 45.º, n.º 2, do Regulamento aprovado), ao ponto de parecer que o TJUE os teve em consideração quando tomou a sua decisão.

Segundo Domingos Soares Farinho, ao analisar a lei de protecção de dados pessoais de um país terceiro para posteriormente qualificá-la numa decisão, a Comissão deverá obrigatoriamente verificar a existência de normas que restrinjam possíveis ingerências nos direitos fundamentais dos particulares cujos dados sejam transferidos da UE para os EUA à estrita medida do necessário, inclusive quando estejam em causa a segurança nacional e o interesse público. [95]

O acesso generalizado ao conteúdo das comunicações electrónicas não deve ser admitido, bem como a conservação dos dados pessoais transferidos da UE para o país terceiro sem qualquer diferenciação em função do objectivo pretendido e sem que haja um critério objectivo que possibilite a delimitação do acesso e posterior uso dos dados por parte das autoridades públicas para fins

[95] FARINHO, Domingos Soares, "(Un)Safe Harbour: Comentário à Decisão do TJUE C-362/14 e suas Consequências Legais", *Fórum de Proteção de Dados*, n.º 2, Janeiro de 2016. Pp. 109 – 124.

que sejam estritamente susceptíveis de justificar essa ingerência. Um regulamento que contenha tais opções é lesivo dos direitos à protecção de dados pessoais e de respeito pela vida privada e familiar, como consagrados nos arts. 6.º e 7.º da Carta.

Garantias de acesso, rectificação e supressão dos dados pessoais ao cidadão europeu a que esses digam respeito deverão igualmente ser asseguradas pelo país terceiro, em virtude da sua legislação interna ou dos compromissos internacionais assumidos, para que a Comissão possa considerar como adequado o nível de protecção existente nesse país.

4.3.3. Validade das Cláusulas Contratuais-Tipo como Base Legal para as Transferências Transatlânticas de Dados Pessoais

A principal consequência do acórdão do TJUE foi a de que o *High Court* deveria impor ao Comissário irlandês para a Protecção de Dados que proceda à análise da queixa de Schrems e que esclareça se será imperativo suspender a transferência dos dados dos assinantes europeus do *Facebook* para os EUA em razão de esse país não oferecer um nível de protecção adequado de dados pessoais. [96]

Tal veio a acontecer a 20 de Outubro de 2015, quando, na audiência final que concluiu o processo, o *High Court* anulou o arquivamento da queixa de Schrems, ordenando o Comissário a investigar os factos aí denunciados.

Como ficou expresso no acórdão do TJUE, a então vigência da Decisão "Porto Seguro*"* não podia ser utilizada como argumento para justificar a recusa do Comissário em examinar as críticas de Schrems quanto ao nível de protecção dos dados pessoais dos cidadãos europeus que é assegurado pelo direito norte-americano. Perante isto, e uma vez que a decisão de adequação em causa foi declarada inválida, o Comissário está obrigado a proceder a uma investigação que, com base nas acusações formuladas na queixa e com a devida diligência, esclareça se os fluxos de dados da filial europeia do

[96] TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA, Comunicado de Imprensa n.º 117/15, Luxemburgo, 6 de Outubro de 2015. Disponível em http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117pt.pdf (data da consulta: 05-01-2017).

Facebook Inc. para a sede norte-americana violam ou não as normas europeias em matéria de protecção de dados pessoais.

Dada a Decisão "Porto Seguro" ter sido considerada inválida, Schrems actualizou o conteúdo original da sua queixa. [97] No texto que enviou ao Comissário, o activista austríaco contesta o facto de o *Facebook Ireland* continuar a transferir os dados pessoais que obtém para os EUA, mas agora assente nas cláusulas contratuais-tipo.

Dessa forma, segundo Schrems, o acesso ilegítimo das autoridades norte-americanas aos dados pessoais dos cidadãos europeus mantém-se, pelo que apela ao Comissário que suspenda todos os fluxos de dados existentes entre o *Facebook Ireland* e o *Facebook Inc.*

A 25 de Maio de 2016, numa nota dirigida à imprensa, o grupo *Europe versus Facebook*, fundado por Schrems, comunicou que o Comissário pretende remeter para o TJUE a questão de saber se o *Facebook Ireland* pode continuar a transferir os dados pessoais da UE para a sede norte-americana com recurso a cláusulas contratuais-tipo, à semelhança de outras empresas, que optaram por esse mecanismo após a Decisão *"Porto Seguro"* ter sido declarada inválida. [98]

Ao pretender o envolvimento do TJUE no esclarecimento sobre o estatuto jurídico das cláusulas contratuais-tipo, o Comissário visa clarificar se tais instrumentos jurídicos protegem adequadamente os titulares dos dados de qualquer actuação das autoridades norte-americanas que seja contrária aos valores europeus de protecção de dados pessoais e de respeito pela vida familiar e pela intimidade. Dado não lhe ser permitido dirigir-se directamente ao TJUE, o Comissário interpôs recurso para o *High Court,* para que este suspenda o processo nacional e submeta ao TJUE as questões relativas à

[97] SCHREMS, Maximilian, "Complaint against Facebook Ireland Ltd", Viena, 1 de Dezembro de 2015. Disponível em http://www.europe-v-facebook.org/comp_fb_ie.pdf (data da consulta: 05-01-2017).

[98] EUROPE VERSUS FACEBOOK, "Rapid Press Update: Facebook & NSA-Surveillance: Following "Safe Harbor" decision, Irish Data Protection Commissioner to bring EU-US data flows before CJEU again", *Europe versus Facebook*, 25 de Maio de 2016, 2.ª versão. Disponível em http://www.europe-v-facebook.org/PA_MCs.pdf (data da consulta: 05-01-2017).

validade das cláusulas contratuais-tipo, enquanto meio utilizado para os fluxos transatlânticos de dados pessoais. [99]

No mesmo comunicado de 25 de Maio de 2016, o grupo *Europe versus Facebook* afirmou que, em um projecto de decisão não publicado, o Comissário apoia Schrems nas suas objecções contra o *Facebook Inc.,* ou seja, que a empresa está sujeita às leis norte-americanas de vigilância em massa e que os dados pessoais dos cidadãos europeus, uma vez recebidos, são alvo de um tratamento que viola os direitos fundamentais, consagrados na legislação comunitária, de respeito pela vida familiar e intimidade e de protecção de dados pessoais. [100]

Dadas as consequências que o caso pode ter para as autoridades e empresas norte-americanas, o Governo dos EUA solicitou ao *High Court* a intervenção como *amicus curiae*[101]*,* expressão latina que designa o terceiro que integra um processo com o intuito de fornecer informações relevantes para a discussão do caso, contribuindo para que o tribunal tenha uma visão mais abrangente sobre o objecto do processo e tome, assim, uma decisão mais justa.

No total, se contarmos com o Governo dos EUA, foram onze as entidades que manifestaram ao tribunal a sua pretensão de participarem como *amici curiae.* Entre essas estão grupos que representam as companhias da indústria tecnológica, como a *The American Chamber of Commerce*, a *Business Software Alliance*, *a Digital Europe* e a *Irish Business and Employers Confederation*, [102] cujos pedidos devem-se ao facto de os membros dessas organizações utilizarem a mesma base legal que o *Facebook Ireland* para transferirem dados pessoais da UE para os EUA, tendo, portanto, interesse no

[99] Art. 267.º, al. *a)*, do Tratado sobre o Funcionamento da União Europeia.
[100] *EUROPE VERSUS FACEBOOK*, "US data flows before CJEU again", *Europe versus Facebook,* 25 de Maio, 2.ª versão. Disponível em http://www.europe-v-facebook.org/PA_MCs.pdf (data da consulta: 05-01-2017).
[101] CAROLAN, Mary, "US government wants to be joined in Schrems case", *The Irish Times*, 13 de Junho de 2016. Disponível em http://www.irishtimes.com/business/technology/us-government-wants-to-be-joined-in-schrems-case-1.2683066 (data da consulta: 05-12-2016).
[102] EUROPE VERSUS FACEBOOK, "NSA Mass Surveillance: US Government wants to intervene in European Facebook-Case", *Europe versus Facebook,* 13 de Junho de 2016. Disponível em http://www.europe-v-facebook.org/PR_MC-US.pdf (data da consulta: 05-01-2017).

resultado do processo. As restantes seis são constituídas por organizações que defendem os direitos humanos e as liberdades civis, como é o caso da *Electronic Frontier Foundation*, *Electronic Privacy Information Center (EPIC)*, *Irish Council for Civil Liberties, American Civil Liberties Union* e da *Irish Human Rights and Equality Commission*, bem como pelo autor e jornalista Kevin Cahill. [103]

O elevado número de pedidos de participação como *amicus curiae* reflecte a crescente importância que os fluxos de dados têm para os governos e empresas dos dois lados do Atlântico, pelo que é do seu interesse que o recurso às cláusulas contratuais-tipo, que permitiu a manutenção dessas transferências após a declaração de invalidade da Decisão "Porto Seguro", continue a ser possível. De acordo com os cálculos da *Business Software Alliance*, se as cláusulas contratuais-tipo forem consideradas inválidas, tal decisão terá um impacto negativo de cerca de um por cento do PIB europeu, o que representa um custo anual para a UE na ordem dos 143 biliões de euros.[104]

No caso específico do Governo dos EUA, o requerimento para a sua inclusão como *amicus curiae* no litígio que opõe Schrems e o Comissário tem como objectivo o de poderem demonstrar que os tribunais europeus interpretam erradamente as práticas dos serviços de segurança norte-americanos, negando, assim, que os dados pessoais transferidos da União Europeia sejam alvo de um programa de vigilância indiscriminado.

A 19 de Julho de 2016, o *High Court* deferiu o pedido do Governo dos EUA de ser integrado no processo com o estatuto de *amicus curiae*. Quanto às outras entidades que solicitaram igualmente a sua inclusão no litígio como

[103] RTÉ NEWS, "Commercial Court hears US government arguments for involvement in data protection case", *RTÉ News*, 7 de Julho de 2016. Disponível em http://www.rte.ie/news/2016/0707/800815-facebook-data-commissioner/ (data da consulta: 05-01-2017).
[104] CAROLAN, Mary, "Ruling against data transfer regime may cost Europe €143bn a year, says Facebook", *The Irish Times,* 7 de Julho de 2016. Disponível em http://www.irishtimes.com/business/technology/ruling-against-data-transfer-regime-may-cost-europe-143bn-a-year-says-facebook-1.2713685 (data da consulta: 05-01-2017).

amici curiae, apenas foram aprovados pelo tribunal os pedidos da *Electronic Privacy Information Center, Business Software Alliance* e da *Digital Europe*. [105]

O *High Court* definiu 7 de Fevereiro de 2017 como a data em que será conhecida a sua decisão quanto ao recurso, apresentado pelo Comissário, referente à validade das cláusulas contratuais-tipo como a base legal para a transferência transatlântica de dados pessoais. Caso considere que os argumentos alegados pelo Comissário são legítimos, o tribunal procederá ao envio das questões em apreço ao TJUE para que este avalie se tais fluxos de dados estão conformes ao direito da União. Se a resposta for negativa, o TJUE declarará a invalidade das cláusulas contratuais-tipo como fundamento legal para a transferência de dados pessoais dos cidadãos europeus para os EUA.[106]

[105] EUROPE VERSUS FACEBOOK, "US government joins Facebook EU-US data transfer case as "amicus"", *Europe versus Facebook,* 19 de Julho de 2016. Disponível em http://www.europe-v-facebook.org/PA_AJ.pdf (data da consulta: 05-01-2017).

[106] CAROLAN, Mary, "Schrems and Facebook privacy case: next round set for February", *The Irish Times*, 25 de Julho de 2016. Disponível em http://www.irishtimes.com/business/technology/schrems-and-facebook-privacy-case-next-round-set-for-february-1.2733961 (data da consulta: 05-01-2017).

5. UM NOVO ACORDO TRANSATLÂNTICO: O "ESCUDO DE PROTECÇÃO DA PRIVACIDADE UE-EUA" (*EU-U.S. PRIVACY SHIELD*)

5.1. Enquadramento Geral

Das negociações entre a Comissão e os EUA para um renovado enquadramento para a migração transatlântica de dados pessoais surge o designado "Escudo de Protecção da Privacidade UE-EUA" (*"EU-U.S. Privacy Shield",* no original), aprovado a 2 de Fevereiro de 2016 pela Comissão.

O projecto de decisão de adequação, bem como os textos jurídicos que procederam a criação do "Escudo de Protecção da Privacidade UE-EUA", foram tornados públicos pela Comissão a 29 de Fevereiro de 2016.[107] Paralelamente, apresentou uma Comunicação[108] onde sintetiza os progressos feitos para restabelecer a confiança no intercâmbio de dados pessoais entre os EUA e a UE no seguimento das revelações sobre a existência de um programa de vigilância norte-americano em larga escala, que abrangia dados dos cidadãos europeus, e da anulação da Decisão "Porto Seguro" pelo TJUE no Acórdão Schrems, em consonância com as Orientações Políticas da Comissão Juncker.[109]

Na sequência da conclusão das negociações da UE com os EUA para um novo quadro transatlântico para o fluxo de dados pessoais, nas quais deram origem ao "Escudo de Protecção da Privacidade UE-EUA", a Comissão ficou encarregue de apresentar o acordo alcançado ao Grupo de Trabalho do art. 29.º, para que esta se pronuncie, através de um parecer, sobre o nível de protecção previsto, sendo que a AEPD deverá ser igualmente consultada antes de a decisão final ser adoptada pelo Colégio dos Comissários. Quanto à

---

[107] COMISSÃO EUROPEIA, Comunicado de imprensa "Restabelecer a confiança nas transferências transatlânticas de dados através de sólidas garantias: Comissão Europeia apresenta Escudo de Privacidade UE-EUA", Bruxelas, 29 de Fevereiro de 2016. Disponível em: http://europa.eu/rapid/press-release_IP-16-433_pt.htm (data da consulta: 05-01-2017).

[108] COMISSÃO EUROPEIA, "Comunicação da Comissão ao Parlamento Europeu e ao Conselho - Transferência transatlântica de dados: restaurar a confiança através de garantias sólidas", COM(2016) 117 final, Bruxelas, 29 de Fevereiro de 2016.

[109] JUNCKER, Jean-Claude, "Um novo começo para a Europa: o meu Programa para o emprego, o crescimento, a equidade e a mudança democrática", Estrasburgo, 15 de Julho de 2014. Pp. 9 – 10. Disponível em https://ec.europa.eu/priorities/sites/beta-political/files/juncker-political-guidelines-speech_pt.pdf (data da consulta: 05-01-2017).

correspondente decisão de adequação, a sua admissão seguiu o procedimento de comitologia previsto.[110]

Depois de o Grupo de Trabalho do Art. 29.º e a AEPD [111] terem expressado a sua posição sobre o "Escudo de Protecção da Privacidade UE-EUA", bem como o Parlamento Europeu através da adopção de uma resolução[112], o processo para a adopção do novo acordo exigiu que previamente o Comité do Art. 31.º pronunciasse sobre o seu conteúdo.

Composto por representantes dos diferentes Estados-Membros e presidido pelo representante da Comissão, o Comité do Art. 31.º é um órgão consultivo que tem como função apreciar os projectos de medidas a adoptar que lhe sejam submetidos pelo representante da Comissão, sendo que emite posteriormente um parecer sobre esse projecto.[113]

Por estar em causa a possível adopção de um projecto de decisão de adequação, foi aplicado o procedimento de exame.[114] Por esta razão, o parecer teve que ser aprovado por maioria qualificada, ou seja, por 16 dos 28 representantes dos Estados-Membros, devendo estes constituir, no mínimo, 65% da população da UE.[115]

Caso o Comité do Art. 31.º recusasse dar o seu aval ao "Escudo de Protecção da Privacidade UE-EUA", a Comissão ficaria impedida de adoptar o novo acordo.[116] Assim, o Colégio de Comissários, que compõe a Comissão, teve que aguardar pela apreciação do Comité do Art. 30.º. Com quatro

[110] O termo "comitologia" é utilizado para designar a forma como a Comissão exerce as competências de execução que lhe são legalmente atribuídas, com o auxílio de comités de representantes dos Estados-Membros.
[111] Os pareceres do Grupo de Trabalho do Art. 29.º e da AEPD serão analisados, respectivamente, no quarto e quinto subcapítulos do Capítulo 5.
[112] A resolução adoptada pelo Parlamento Europeu será estudada no sexto subcapítulo do Capítulo 5.
[113] Art. 31.º da Directiva.
[114] Art. 2.º, n.º 2, al. a), do Regulamento (UE) n.º 182/2011 de 16 de Fevereiro de 2011.
[115] Art. 5.º, n.º 1, do Regulamento (UE) n.º 182/2011 de 16 de Fevereiro de 2011 e art. 16.º, n.º 4, do Tratado da UE.
[116] Art. 5.º, n.º 3, e art. 7.º do Regulamento (UE) n.º 182/2011 de 16 de Fevereiro de 2011.

abstenções dos representantes dos países que o constituem[117], o "Escudo de Protecção da Privacidade UE-EUA" foi aprovado a 8 de Julho de 2016.

Uma vez que o parecer foi favorável, o "Escudo de Protecção da Privacidade UE-EUA" pôde, então, ser adoptado pelo Colégio de Comissários.[118] Tal veio a acontecer a 12 de Julho de 2016[119], finalizando um longo processo que culminou na aprovação do acordo alcançado como a nova base legal para as transferências de dados pessoais dos cidadãos europeus para as empresas norte-americanas que subscrevam e respeitem os princípios e compromissos aí consagrados.

A aprovação foi notificada aos Estados-Membros, entrando imediatamente em vigor no espaço europeu. Nos EUA, os textos que fazem parte do "Escudo de Protecção da Privacidade UE-EUA" foram publicados a 2 de Agosto de 2016 no *U.S. Federal Register*, o jornal oficial do governo federal norte-americano.[120]

Nesse contexto, foi estabelecido que as empresas que pretendam recorrer ao novo sistema deverão obter uma certificação junto do Departamento de Comércio a partir do dia 1 de Agosto, após examinarem e adequarem-se às condições previstas para a circulação de dados pessoais.

Com o propósito de proporcionar um melhor esclarecimento sobre as vias de recursos disponíveis no novo acordo, a Comissão publicou ainda um guia sucinto dirigido aos cidadãos europeus que queiram recorrer a essas vias,

---

[117] Áustria, Bulgária, Croácia e Eslovénia. Ver CELULUS, Laurens, "Companies get data transfer safety net — for now", 8 de Julho de 2016. Disponível em http://www.politico.eu/article/privacy-shield-adoption-eu-countries-national-experts-safe-harbor-data-transfers/) (data da consulta: 05-01-2017).

[118] Art. 5.º, n.º 2, do Regulamento (UE) n.º 182/2011 de 16 de Fevereiro de 2011.

[119] Decisão de Execução (UE) 2016/1250 da Comissão, de 12 de Julho de 2016.

[120] INTERNATIONAL TRADE ADMINISTRATION, DEPARTMENT OF COMMERCE, "Notice of Availability of Privacy Shield Framework Documents", *Federal Register,* Vol. 81, n.º 148, Office of the Federal Register, 2 de Agosto de 2016. Pp. 51042 – 51074. Disponível em https://www.gpo.gov/fdsys/pkg/FR-2016-08-02/pdf/2016-17961.pdf (data da consulta: 05-01-2017).

por considerarem que houve uma utilização dos seus dados pessoais que desobedece às regras consagradas em matéria de protecção de dados.[121]

Por seu lado, o Departamento do Comércio, em conjunto com a *International Trade Administration,* lançaram um *site*[122] com informações relevantes para as empresas norte-americanas e europeias, particulares e agências nacionais de controlo sobre o funcionamento do novo acordo. É ainda possível, através desse *site*, consultar as empresas que aderiram.

Porém, os pedidos de clarificações e melhorias adicionais a vários aspectos do "Escudo de Protecção da Privacidade UE-EUA", presentes nos pareceres do Grupo de Trabalho do artigo 29.º e da AEPD, bem como na resolução do Parlamento Europeu, não foram esquecidos. Neste sentido, tanto a Comissão como os EUA comprometeram-se a elaborar esclarecimentos adicionais sobre os tópicos mais controversos do novo acordo, nomeadamente a recolha de dados em larga escala, o papel e os poderes do mediador e os limites que se impõem às empresas para a conservação e transferência posterior dos dados. [123]

5.2. Principais Aspectos

5.2.1. Mecanismos de Supervisão e de Aplicação

Com a pretensão de reflectir as exigências expressas no Acórdão Schrems, foram ampliadas as regras relativamente à protecção dos dados pessoais dos cidadãos europeus que as empresas norte-americanas têm que obedecer quando procedem à transferência e posterior tratamento desses dados, de forma a garantir o respeito pelos direitos fundamentais dos titulares dos dados.

Para assegurar a real efectividade dessas regras, o Departamento do Comércio terá uma maior capacidade de supervisão do cumprimento dos

[121] COMISSÃO EUROPEIA, "Guide to the EU-U.S. Privacy Shield", 2016. Disponível em http://ec.europa.eu/justice/data-protection/files/eu-us_privacy_shield_guide_en.pdf (data da consulta: 05-01-2017).
[122] https://www.privacyshield.gov
[123] COMISSÃO EUROPEIA, Comunicado de imprensa "A Comissão Europeia lança o Escudo de Proteção da Privacidade UE-EUA: uma maior proteção para a transferência transatlântica de dados", Bruxelas, 12 de Julho de 2016. Disponível em http://europa.eu/rapid/press-release_IP-16-2461_pt.htm (data da consulta: 05-01-2017).

compromissos assumidos publicamente pelas empresas norte-americanas, visto que estes autocertificam a sua adesão aos princípios do "Escudo de Protecção da Privacidade UE-EUA"[124] junto do Departamento do Comércio.[125] É da sua competência verificar sistematicamente se as políticas das organizações em matéria de protecção de dados observam os referidos princípios, no contexto da certificação e renovação da certificação da adesão da empresa ao quadro. [126]

Por força do novo acordo, as organizações que participem no "Escudo de Protecção da Privacidade UE-EUA" estarão sujeitas aos poderes de investigação e de execução da Comissão Federal do Comércio, que averiguará se essas empresas declararam publicamente o seu compromisso em cumprir os princípios, divulgaram manifestamente as suas políticas de protecção da privacidade em conformidade com estes princípios e, por fim, se os aplicam na íntegra.[127] No caso de a existência de tais práticas desleais e enganosas[128] se confirmar, pode impor à organização em causa a modificação da sua conduta através de uma decisão administrativa ("injunção") ou, se esta não for cumprida, submeter o caso ao tribunal competente com o intuito de solicitar sanções de carácter civil e outras reparações.[129]

A Comissão Federal do Comércio deverá exercer os seus poderes com base numa queixa submetida por um organismo independente de resolução de litígios ou de auto-regulação, pelo Departamento do Comércio e pelas autoridades nacionais de controlo, ainda que os particulares lhe possam apresentar directamente queixa. No entanto, é-lhe permitido investigar por iniciativa própria no âmbito das suas investigações de grande dimensão sobre questões relacionadas com a privacidade. [130]

Prevê-se ainda o reforço da cooperação entre as autoridades norte-americanas e as autoridades europeias de controlo em matéria de protecção de dados, com o Departamento do Comércio encarregado de estabelecer um

[124] Anexo II do "Escudo de Protecção da Privacidade UE-EUA", secção II.
[125] Considerando (14) do "Escudo de Protecção da Privacidade UE-EUA".
[126] Considerando (32) do "Escudo de Protecção da Privacidade UE-EUA".
[127] Considerando (54) do "Escudo de Protecção da Privacidade UE-EUA".
[128] Nos termos da secção 5 do *Federal Trade Commission Act*.
[129] Considerando (55) do "Escudo de Protecção da Privacidade UE-EUA".
[130] Considerando (54) do "Escudo de Protecção da Privacidade UE-EUA".

"ponto de contacto específico" que sirva de ligação com as autoridades nacionais de protecção de dados e assisti-las nas investigações relativas à observância dos princípios por parte de uma organização quando lhes seja apresentada queixa.[131] De referir que as empresas são obrigadas a cooperar com as autoridades nacionais de protecção de dados na investigação e resolução de uma queixa se esta for referente ao tratamento de dados de recursos humanos obtidos em contexto laboral ou se a entidade em questão se tiver sujeitado voluntariamente à supervisão das autoridades nacionais.[132]

5.2.2. Limitação do Acesso aos Dados Transferidos por parte das Autoridades Norte-Americanas

A fim de limitar o acesso para efeitos de segurança nacional das autoridades públicas norte-americanas aos dados pessoais que tenham sido transferidos da União Europeia, os EUA deram garantias de que, a acontecer, será sempre na medida do necessário e sujeito às condições e limitações previstas.

Quando procedam à recolha de dados pessoais proveniente da UE, os serviços de informação norte-americanos estão vinculados aos limites estabelecidos pela *Presidential Policy Directive 28*.[133] De acordo com este instrumento jurídico, a obtenção de informações com essas características deve basear-se numa lei ou autorização presidencial e ser efectuada de acordo com a Constituição (em particular, a Quarta Emenda) e a legislação dos EUA. Cumulativamente, deve assegurar o respeito pela dignidade e privacidade do titular dos dados. [134]

Os serviços de informação norte-americanos devem ainda dar prioridade a uma recolha selectiva de dados, dada ser a que melhor salvaguarda os direitos dos cidadãos europeus. Porém, caso aquela não se possa realizar por

[131] Considerando (51) do "Escudo de Protecção da Privacidade UE-EUA".
[132] Considerando (49) do "Escudo de Protecção da Privacidade UE-EUA"
[133] Emitida a 17 de Janeiro de 2014, a *Presidential Policy Directive 28* estabelece uma série de princípios e requisitos aplicáveis a todas as actividades de "informação de origem electromagnética" dos EUA, sendo vinculativa para os serviços de informação norte-americanos. Em particular, determina os requisitos aplicáveis aos procedimentos para lidar com a recolha, a preservação e a divulgação de dados pessoais dos cidadãos de países terceiros que tenham sido obtidos através de operações de "informação de origem electromagnética".
[134] Considerando (69) do "Escudo de Protecção da Privacidade UE-EUA"

motivos técnicos ou operacionais, a recolha em larga escala é admitida desde que a utilização posterior dos dados obtidos seja estritamente limitada a objectivos de segurança nacional específicos e legítimos. [135] Entre as seis finalidades que justificam uma recolha de dados com essa dimensão, constam: a detenção e combate a determinadas actividades de potências estrangeiras; a luta contra o terrorismo; a luta contra a proliferação; a *cyber*segurança; a detenção e combate a ameaças para os EUA e os seus aliados; e o combate às ameaças criminosas transnacionais, como evasões ou sanções. [136]

Tais dados estão ainda excluídos de qualquer programa de vigilância indiscriminada ou em massa, ainda que justificada por fins de segurança interna, por parte das entidades estatais norte-americanas.[137] Pretende-se, com estas medidas, afastar a possibilidade de um acesso indiferenciado aos dados pessoais dos cidadãos europeus, precisamente um dos argumentos invocados pelo TJUE para justificar a sua declaração de invalidade da Decisão "Porto Seguro" no Acórdão Schrems. [138]

5.2.3. Novas Vias de Recurso

Para garantir igualmente uma protecção mais eficaz dos direitos dos cidadãos europeus, estes terão à sua disposição, com o novo acordo, diversos mecanismos de recurso contra o tratamento irregular ou ilícito dos seus dados.

É exigido que as empresas responsáveis pelo tratamento dos dados respondam às reclamações apresentadas pelos titulares dos dados no prazo de 45 dias, independentemente de a queixa ter sido apresentada directamente pelo interessado ou através do Departamento do Comércio na sequência de um reenvio por uma autoridade responsável pela protecção de dados. [139] De modo a facilitar que os titulares dos dados entrem em contacto directo com as empresas autocertificadas norte-americanas nos casos de incumprimento dos princípios do "Escudo de Protecção da Privacidade UE-EUA", as referidas organizações devem informar nas suas políticas de protecção da privacidade

[135] Considerandos (71) e (76) do "Escudo de Protecção da Privacidade UE-EUA"
[136] Anexo VI do "Escudo de Protecção da Privacidade UE-EUA", secção I, al. *b)*. P. 3.
[137] *Idem*. P. 5.
[138] Acórdão Schrems §93, 98 e 105.
[139] Considerando (44) do "Escudo de Protecção da Privacidade UE-EUA".

qual a entidade, interna ou externa à empresa, que procederá à resolução das queixas e quais os mecanismos de recurso independentes que existem. [140]

Os cidadãos europeus poderão recorrer igualmente a um organismo independente para a resolução de litígios, que será designado pela empresa autocertificada e poderá estar sediado nos EUA ou na UE. Está prevista a hipótese de esse organismo poder consistir num painel instituído pelas autoridades europeias responsáveis pela protecção de dados. [141] As sanções e reparações que imponha devem ser consideradas *"suficientemente rigorosas"* para garantir que as empresas actuam em conformidade com os princípios de protecção da privacidade consagrados, devendo mencionar o que está ao alcance das organizações para inverterem ou corrigirem os efeitos do incumprimento e em que circunstâncias se deve avançar para a cessação da continuação do tratamento de dado em causa e/ou a sua eliminação. [142]

Nos casos em que tenham sido esgotadas todas as vias de recurso e nenhuma dela tenha resolvido a queixa de modo satisfatório, o seu autor tem o direito de invocar uma arbitragem vinculativa ao abrigo do Comité do Escudo de Protecção da Privacidade. [143] As partes poderão seleccionar dois a três dos árbitros[144] que estejam previstos numa lista elaborada pelo Departamento do Comércio e pela Comissão e na qual deverão constar, pelo menos, vinte juízes.[145] Os árbitros, escolhidos conforme a vontade das partes, têm competência para aplicarem somente medidas que sejam *"equitativas, não monetárias e específicas do cidadão (tais como acesso, correcção, eliminação ou devolução dos dados do cidadão em questão)"* e consideradas essenciais para cessar a situação de incumprimento dos princípios que prejudica o particular. [146]

[140] Considerando (43) do "Escudo de Protecção da Privacidade UE-EUA".
[141] Anexo II do "Escudo de Protecção da Privacidade UE-EUA", secção II, n.º 1, al. *a)*, subalínea *ix)*.
[142] Considerando (45) do "Escudo de Protecção da Privacidade UE-EUA".
[143] Anexos 1 e 2 da Decisão de Execução do "Escudo de Protecção da Privacidade UE-EUA".
[144] Anexo 2 da Decisão de Execução do "Escudo de Protecção da Privacidade UE-EUA", anexo I, B.
[145] *Idem*, anexo I, F.
[146] *Idem*, anexo I, B.

5.2.4. Mediador para o Escudo de Protecção da Privacidade

Em carta assinada pelo então Secretário de Estado John Kerry e que figura no anexo III da decisão aprovada, foi assumido o compromisso de criar um novo mecanismo de supervisão: o Mediador para o Escudo de Protecção da Privacidade (doravante, «mediador»), cujas funções serão desempenhadas por um coordenador superior do Departamento de Estado e junto do qual os governos estrageiros poderão *"expressar preocupações sobre as actividades de informação de origem electromagnética dos EUA"*.[147]

Enquanto órgão independente dos serviços de informação norte-americanos, esse mecanismo assegurará ainda que as queixas individuais relativas a ingerências das autoridades públicas dos EUA nos dados transferidos são investigadas e abordadas adequadamente. No final da sua investigação, deverá confirmar se as leis norte-americanas foram cumpridas ou, no caso de não terem sido, se o incumprimento foi corrigido. [148]

Para o exercício das suas funções, o mediador poderá solicitar a cooperação de outros mecanismos de verificação do cumprimento e de supervisão previstos na legislação dos EUA.[149]

Os cidadãos europeus terão a opção de apresentarem as suas queixas às autoridades nacionais de controlo em matéria de protecção de dados, que, por sua vez, irão remete-las a um organismo centralizado a nível europeu cuja tarefa será a de enviá-las ao mediador. Tal beneficiará os particulares que queiram recorrer a este mecanismo para contestar um acesso ilícito dos serviços de informação norte-americanos aos seus dados pessoais, já que poderão se dirigir directamente à autoridade nacional de controlo do seu país, que deverá dar o apoio necessário para que o pedido seja tão completo quanto possível. [150]

---

[147] Considerandos (65) e (116) do "Escudo de Protecção da Privacidade UE-EUA" e Anexo A, secção 1, do Anexo III do "Escudo de Protecção da Privacidade UE-EUA".
[148] Considerando (117) do "Escudo de Protecção da Privacidade UE-EUA" e Anexo A, secção 2, do Anexo III do "Escudo de Protecção da Privacidade UE-EUA".
[149] Considerando (118) do "Escudo de Protecção da Privacidade UE-EUA" e Anexo A, secção 3, do Anexo III do "Escudo de Protecção da Privacidade UE-EUA".
[150] Considerando (119) do "Escudo de Protecção da Privacidade UE-EUA" e Anexo A, secção 3, do Anexo III do "Escudo de Protecção da Privacidade UE-EUA".

5.2.5. Reapreciação Periódica da Verificação de Adequação

Dado que o nível de protecção conferido pela legislação norte-americana é susceptível de sofrer alterações após a entrada em vigor do "Escudo de Protecção da Privacidade UE-EUA", ficou estabelecido que a Comissão certificará periodicamente se se mantêm factual e legalmente justificados os fundamentos que a conduziram a considerar como adequado o nível de protecção assegurado pelos EUA. De realçar que tal verificação será obrigatória quando a Comissão receba informações que justificadamente coloquem em causa a apreciação feita. [151]

Para facilitar o acompanhamento da Comissão de qualquer evolução observada na ordem jurídica norte-americana que possa comprometer o pleno funcionamento do novo mecanismo, os EUA deverão informá-la quando procede a modificações legislativas no domínio da protecção dos dados e das limitações e garantias aplicáveis ao acesso das autoridades públicas aos dados pessoais.

Mais relevante, contudo, é o facto de se ter instituído de que o "Escudo de Protecção da Privacidade UE-EUA" deverá ser apreciado anualmente e de forma conjunta pela Comissão, pelo Departamento do Comércio e pela Comissão Federal do Comércio, de modo a garantir a manutenção de um nível de protecção adequado dos dados pessoais nas transferências transatlânticas e a corrigir eventuais falhas detectadas no acordo durante sua vigência.[152] Para tal, e no âmbito desta reunião, a Comissão solicitará que sejam apresentadas informações e esclarecimentos sobre todos os aspectos necessários para a análise do efectivo funcionamento do novo mecanismo.[153]

Na realização da reapreciação conjunta anual a que se referem os anexos I, II e VI, os órgãos envolvidos poderão ser acompanhados por outros departamentos e serviços que apliquem as disposições do novo quadro, assim como, quando estejam em causa questões relativas à segurança nacional, por representantes do *Office of the Director of National Intelligence*, outros

[151] Considerando (145) do "Escudo de Protecção da Privacidade UE-EUA"
[152] Considerando (146) do "Escudo de Protecção da Privacidade UE-EUA"
[153] Considerando (148) do "Escudo de Protecção da Privacidade UE-EUA"

elementos dos serviços de informação norte-americanos e pelo mediador. Esta reunião estará ainda aberta à participação das autoridades nacionais de controlo de protecção de dados e dos representantes do Grupo de Trabalho do Art. 29.º. [154]

Concluída a reapreciação conjunta anual, a Comissão elaborará um relatório público sobre os resultados da reunião com o Departamento do Comércio e a Comissão Federal do Comércio que será apresentado ao Parlamento Europeu e ao Conselho. [155]

5.3. Princípios Gerais

À semelhança do que acontecia com o sistema "Porto Seguro", as empresas norte-americanas que tencionam importar dados pessoais da UE ao abrigo do novo quadro terão que se comprometer a cumprir um conjunto de princípios gerais referente à protecção da privacidade dos titulares dos dados, emitidos pelo Departamento do Comércio e que constam no anexo II da decisão adoptada. Além desses, terão ainda que respeitar os designados princípios suplementares.[156]

5.3.1. Princípio do Aviso

O princípio do aviso impõe às organizações o dever de informar os particulares em causa sobre os aspectos essenciais relativos ao tratamento dos seus dados pessoais, obrigando de igual modo, por força desse princípio, as empresas a divulgarem as suas políticas de privacidade e a fornecerem ligações ao *website* do Departamento do Comércio, ao texto do "Escudo de Protecção da Privacidade EU-EUA" e ao *website* da resolução alternativa de litígios mais apropriada para o caso. [157]

---

[154] Considerando (147) do "Escudo de Protecção da Privacidade UE-EUA"
[155] Considerando (148) do "Escudo de Protecção da Privacidade UE-EUA"
[156] Anexo II do "Escudo de Protecção da Privacidade EU-EUA", secção III. Entre os princípios suplementares constam os referentes: aos dados sensíveis; às excepções jornalísticas; à responsabilidade subsidiária; à realização de auditorias e auditorias jurídicas; ao papel das autoridades responsáveis pela protecção dos dados; à auto-certificação; à verificação; ao acesso; aos dados relativos a recursos humanos; aos contractos obrigatórios para transferências ulteriores; à resolução de litígios e aplicação; etc.
[157] Anexo II do "Escudo de Protecção da Privacidade EU-EUA", secção II, ponto 1, alíneas *a)* e *b)*,

5.3.2. Princípio da Escolha

O princípio da escolha implica que aos particulares seja dada a possibilidade de se oporem à divulgação dos seus dados a terceiros ou a uma utilização desses para um propósito "substancialmente diferente" ao que era inicialmente previsto. Quando estejam em causa dados considerados sensíveis, as empresas devem, em princípio, obter o consentimento expresso do titular em questão quando pretendam utilizar esses dados.[158]

5.3.3. Princípio da Responsabilização pela Transferência Ulterior

Por força deste princípio, a transferência ulterior de dados pessoais para um terceiro que irá desempenhar as funções de gestão e tratamento desses dados só pode ocorrer sob três condições: primeira, destinar-se a fins específicos e limitados; segunda, assentar num contrato ou num acordo dentro do mesmo grupo empresarial; terceira, estar garantido, por esse contrato, a continuidade da protecção das informações pessoais em conformidade com os princípios, o que inclui a obrigação de só restringir a aplicação dos princípios na medida do necessário por razões de segurança nacional, de aplicação da lei ou de outros interesses públicos.

Este princípio deve ainda ser examinado em conjunto com os princípios do aviso e da escolha, no sentido em que os titulares dos dados devem ser informados da identidade do destinatário terceiro, da finalidade da transferência ulterior e da possibilidade de poderem opor-se ou, no caso de se tratar de dados sensíveis, terem que consentir expressamente a realização dessas transferências. [159]

No contrato celebrado para a transferência ulterior, deve constar que o destinatário terceiro notificará a organização se considerar já não poder cumprir com a obrigação de assegurar o mesmo nível de protecção exigido pelos princípios, devendo ainda cessar o tratamento de dados ou tomar as medidas necessárias para resolver a situação.[160]

---

[158] Anexo II do "Escudo de Protecção da Privacidade EU-EUA", secção II, ponto 2, alíneas *a)* e *c)*,
[159] Considerando (28) do "Escudo de Protecção da Privacidade EU-EUA".
[160] Anexo II do "Escudo de Protecção da Privacidade EU-EUA", secção II, ponto 3, al. *a)*,

5.3.4. Princípio da Segurança

Este princípio consiste na exigência, dirigida às empresas aderentes, de que estas devem desenvolver mecanismos de segurança considerados razoáveis e apropriados em função dos riscos que a sua actividade envolve para os dados pessoais.[161] No caso de tratamento ulterior, devem, então, celebrar um contrato com a entidade que será responsável por esse tratamento, de forma a garantir que o nível de protecção previsto pelos princípios se mantém e que serão adoptadas as devidas precauções para garantir a sua aplicação adequada. [162]

5.3.5. Princípio da Integridade dos Dados e Limitação dos Fins

No âmbito deste princípio, o tratamento de dados pessoais deve-se restringir àqueles que sejam necessários para alcançar as finalidades pretendidas e fiáveis para a utilização prevista, assim como os que sejam exactos, completos e actuais. Tal significa, portanto, que uma organização está impedida de tratar dados pessoais de um modo incompatível com os fins que justificaram a recolha ou com os objectivos autorizados posteriormente pelo particular em causa. [163]

Ainda segundo o princípio da integridade dos dados e limitação dos fins, os dados só podem ser conservados sob uma forma que possibilite identificar uma pessoa ou a torne identificável (isto é, sob a forma de dados pessoais) durante o tempo em que a sua utilização esteja conforme com os propósitos para os quais foram inicialmente obtidos ou subsequentemente autorizados. [164]

Há que notar, contudo, que esta obrigação não obsta a que as organizações tratem de dados pessoais por períodos mais longos, mas apenas quando seja necessário para a satisfação de fins como o arquivamento no

[161] Anexo II do "Escudo de Protecção da Privacidade EU-EUA", secção II, ponto 4, al. *a)*.
[162] Considerando (24) do "Escudo de Protecção da Privacidade EU-EUA".
[163] Considerando (21) do "Escudo de Protecção da Privacidade EU-EUA".
[164] Considerando (23) do "Escudo de Protecção da Privacidade EU-EUA".

interesse público, a actividade jornalística, literária e artística, a investigação científica ou história e a análise estatística.[165]

5.3.6. Princípio do Acesso

De acordo com este princípio, o particular tem o direito de obter a confirmação, por parte da organização, de que os seus dados pessoais estão a ser por essa processados, sem que lhe seja exigido uma justificação para o exercício desse direito.[166]

Ainda sob este princípio, ao titular deve ser disponibilizado o acesso aos seus dados em tempo útil, bem como a possibilidade de corrigir, modificar ou apagar informações pessoais se estas estiverem incorrectas ou se tiverem sido tratadas num modo que viola os princípios. Qualquer limitação ou negação do seu direito ao acesso só poderá acontecer em casos excepcionais e devidamente fundamentados, cabendo à empresa que o restringiu ou proibiu o ónus de comprovar que tais exigências foram cumpridas. [167]

5.3.7. Princípio do Recurso, Aplicação e Responsabilidade

Segundo este princípio, é obrigatório que as empresas subscritoras do "Escudo de Protecção da Privacidade EU-EUA" desenvolvam os mecanismos adequados para assegurar a conformidade da sua actuação com os princípios, bem como vias de recursos aos cidadãos europeus quando os dados pessoais destes tenham sido processados de um modo contrário ao que é estabelecido na decisão adoptada.

Dado que parte das organizações a iniciativa de auto-certificar a sua adesão ao novo quadro, é-lhes exigido que cumpram de forma efectiva os princípios que aí constam, devendo proceder anualmente à actualização do seu compromisso em aplicá-los nas transferências transatlânticas, para que possam, assim, continuar a receber os dados pessoais dos cidadão europeus no âmbito do acordo aprovado.

---

[165] Anexo II do "Escudo de Protecção da Privacidade EU-EUA", secção II, ponto 5, al. *b)*, De observar que, neste anexo da decisão, o princípio da integridade dos dados e limitação dos fins é referido como o "princípio da integridade dos dados e limitação dos objectivos".
[166] Anexo II do "Escudo de Protecção da Privacidade EU-EUA", secção II, ponto 6, al. *a)*.
[167] Considerando (25) do "Escudo de Protecção da Privacidade EU-EUA".

Do mesmo modo, as empresas devem tomar as medidas necessárias para garantir que as suas políticas de privacidade estão em concordância com os princípios de privacidade e são efectivamente respeitadas. Para tal, pode ser instituído um sistema de auto-avaliação, que deve incluir procedimentos internos em que o cumprimento é revisto periodicamente e de forma objectiva, bem como averiguações de conformidade externas, cujos procedimentos podem envolver auditorias ou verificações aleatórias.

Ademais, as organizações devem desenvolver um mecanismo de recurso efectivo para dar resposta a possíveis queixas, estando submetidas aos poderes de investigação e de execução da Comissão Federal do Comércio, do *Department of Transportation* e de qualquer outra entidade oficial norte-americana que garanta a observância dos princípios.[168] No caso de incumprimento dos princípios por parte de empresa que tenha aderido ao novo quadro, deverá essa ser alvo de sanções consideradas suficientemente rigorosas para forçar a organização a inverter a sua conduta.[169]

5.4. Parecer do Grupo de Trabalho do Art.º 29

No exercício das competências que lhe são atribuídas pelo art. 30.º, n.º 1, al. *c)*, da Directiva, o Grupo de Trabalho do Art.º 29 emitiu um parecer[170] sobre o projecto de decisão de adequação do "Escudo de Protecção da Privacidade UE-EUA", tendo em conta na sua avaliação a legislação da UE aplicável à protecção de dados e a jurisprudência europeia relacionada com os direitos fundamentais ao respeito pela vida privada e familiar e à protecção de dados pessoais, consagrados nos arts. 7.º e 8.º da Carta. Ao proceder à análise do novo acordo, pretendeu certificar-se se um nível essencialmente equivalente de protecção é garantido quando os dados pessoais são tratados no âmbito do novo quadro, isto é, se nele está contida a essência dos princípios fundamentais europeus em matéria de protecção de dados.

---

[168] Considerando (26) do "Escudo de Protecção da Privacidade EU-EUA".

[169] Anexo II do "Escudo de Protecção da Privacidade EU-EUA", secção II, ponto 7, al. *a)*, subalínea *iii).*

[170] GRUPO DE TRABALHO DO ART. 29.º, "Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision", *Working Paper 238,* Bruxelas, 13 de Abril de 2016. Disponível em http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf (data da consulta: 05-01-2017).

No parecer, fez menções elogiosas a vários aspectos do acordo alcançado que procuram colmatar as lacunas da Decisão "Porto Seguro". Entre aqueles que foram referidos estão, nomeadamente, a obrigatoriedade de avaliações regulares e conjuntas entre a Comissão e as autoridades norte-americanas sobre a aplicação prática do novo acordo (podendo as autoridades de protecção de dados participar nessas apreciações através dos seus representantes) e os mecanismos desenvolvidos para assegurar a supervisão do "Escudo de Protecção da Privacidade UE-EUA".

Para além desses elementos, o Grupo de Trabalho destacou ainda os avanços feitos com o princípio do acesso e o reconhecimento dos direitos à rectificação e à eliminação dos dados ao seu titular quando sejam utilizados de um modo incompatível com os princípios de protecção da privacidade do novo acordo, assim como a exigência de confirmar ao particular de que os seus dados estão a ser processados e comunicar-lhe quais os dados que estão nessa situação. Do mesmo modo, saudou o reforço das garantias legais das transferências subsequentes de dados pessoais e os compromissos assumidos pelo Departamento do Comércio e pela Comissão Federal do Comércio de cumprir as obrigações estabelecidas no novo acordo.

No entanto, expressou preocupação com os aspectos comerciais e o acesso das autoridades públicas aos dados pessoais transferidos ao abrigo do novo quadro. Como observação preliminar, manifestou o seu desagrado com o facto de o "Escudo de Protecção da Privacidade UE-EUA" ser constituído por um vasto conjunto de documentos, dificultando a acessibilidade e consistência da informação, o que é demonstrado com a constatação de que os princípios e as garantias asseguradas pelo novo acordo estão definidos tanto na decisão de adequação como nos seus anexos.

Em seguida, no que respeita aos aspectos comerciais, entendeu que alguns dos princípios fundamentais de protecção de dados previstos na legislação europeia não estão reflectidos nos documentos que constituem o "Escudo de Protecção da Privacidade UE-EUA" ou foram inadequadamente substituídos por noções alternativas. Em particular, referiu o princípio da retenção de dados como um dos que não é expressamente mencionado, não

podendo ser deduzido da actual redacção do princípio da integridade dos dados e da limitação da finalidade.

Dado que o novo quadro poderá ser usado para transferir dados pessoais para um país terceiro, o Grupo de Trabalho do Art.º 29 sustentou que em tais transferências ulteriores deve ser assegurado o mesmo nível de protecção previsto pelo novo acordo, sem contornar ou reduzir os princípios europeus de protecção de dados. De um modo geral, considerou que essas transferências não estão devidamente definidas, sobretudo em relação à sua abrangência, limitação de finalidade e às garantias aplicáveis.

Por último, observou que os novos mecanismos de recurso, pela sua complexidade, podem vir a ser de difícil utilização para os cidadãos europeus que queiram exercer os seus direitos, tornando necessário um maior esclarecimento sobre o seu procedimento. A este respeito, sugeriu que as autoridades nacionais de protecção de dados possam ter a opção de actuar em benefício do particular nos processos de recurso quando assim o decidissem.

Relativamente ao acesso das autoridades públicas aos dados pessoais transferidos no âmbito do "Escudo de Protecção da Privacidade UE-EUA", o Grupo de Trabalho do Art.º 29 constatou que os representantes do *U. S. Office of the Director of National Intelligence* não excluíram a hipótese de uma recolha maciça e indiscriminada de dados provenientes da UE, o que, a acontecer, irá contra a exigência de que qualquer acesso aos dados pessoais pelas autoridades públicas tem que ser proporcional ao estritamente necessário para alcançar o objectivo pretendido, sob risco de se estar a violar os direitos fundamentais de respeito pela intimidade e de protecção de dados pessoais. Dada a tendência de justificar a recolha indiscriminada em massa de dados com o combate ao terrorismo, a preocupação com a protecção de tais direitos é, por isso, agravada.

A figura do mediador como um novo mecanismo de recurso, ainda que enaltecida por constituir uma evolução na defesa dos direitos fundamentais do cidadão europeu contra a actividade dos serviços de segurança e inteligência norte-americanos, causou dúvidas quanto à sua independência, visto que o cargo será exercido por um vice-secretário do Departamento de Estado, que

terá que ser nomeado pelo Presidente dos EUA e confirmado pelo Senado Norte-Americano. Dado que será designado para o cargo um dos altos funcionários do Departamento de Estado dos EUA, questionou se será capaz de cumprir os deveres que lhe são atribuídos de modo imparcial, à semelhança do que sucede com os organismos de supervisão independentes que existem em diversos Estados-Membros.

A incerteza quanto à extensão dos poderes de investigação do mediador foi outra das questões expressas no parecer, já que não se esclarece se o mediador pode ter acesso directo aos dados do indivíduo em questão, dirigir a sua própria investigação ou confiar em outros relatórios que não os que sejam produzidos pelos funcionários do governo norte-americano.

Permaneceu igualmente por esclarecer de que forma pode o mediador ordenar a reparação de um acesso aos dados pessoais que tenha sido incompatível com os princípios de protecção de privacidade do "Escudo de Protecção da Privacidade UE-EUA", bem como as consequências que tal decisão acataria. Além disso, notou que não está previsto nenhuma via de recurso em caso de descontentamento com a decisão tomada pelo mediador.

Em suma, embora tenha reconhecido a existência de vários progressos feitos pelo "Escudo de Protecção da Privacidade UE-EUA" em relação à Decisão "Porto Seguro", o Grupo de Trabalho do Art.º 29 apelou à Comissão que fosse dada resposta aos aspectos problemáticos do novo acordo identificados no seu parecer, de modo a conseguir que a protecção assegurada pelo acordo alcançado fosse, de facto, essencialmente equivalente à que está consagrada no direito europeu.

5.5. Resolução do Parlamento Europeu

Na sessão plenária de 25 de Maio de 2016, teve lugar no Parlamento Europeu um debate sobre o conteúdo e a capacidade do "Escudo de Protecção da Privacidade UE-EUA" em restaurar a confiança nos fluxos transatlânticos de

dados pessoais e garantir um nível elevado de protecção dos direitos fundamentais dos titulares dos dados transferidos.[171]

No fim do debate, foram apresentadas sete propostas de resolução pelos diferentes grupos políticos, nos termos do art. 123.º, n.º 2, do Regimento do Parlamento Europeu. Porém, só foram postas à votação na sessão plenária do dia seguinte, isto é, a 26 de Maio de 2016[172], constituindo, portanto, uma excepção à regra, estabelecida no art. 123.º, n.º 3, do Regimento do Parlamento Europeu, de as propostas de resolução terem que ser votadas no mesmo dia do debate.

A primeira proposta de resolução a ir a votos, da autoria do Grupo Verts/ALE[173], foi rejeitada pelo Parlamento Europeu. De seguida, foi apresentada uma proposta de resolução comum[174], em substituição das que tinham sido anteriormente apresentadas pelos Grupos PPE, S&D, ECR, ALDE e EFDD, de acordo com o art. 123.º, n.º 4, do Regimento do Parlamento Europeu. Essa proposta acabou por ser aprovada[175] com 501 votos a favor e 119 votos contra, tendo havido 31 abstenções.[176]

No texto aprovado, após destacarem a importância dos fluxos transfronteiriços de dados entre a UE e os EUA para as relações

---

[171] PARLAMENTO EUROPEU, "Ata da sessão de quarta-feira, 25 de Maio de 2016", Bruxelas. Pp. 12 – 13. Disponível em http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+PV+20160525+SIT+DOC+PDF+V0//PT&language=PT (data da consulta: 05-01-2017).

[172] PARLAMENTO EUROPEU, "Ata da sessão de quinta-feira, 26 de Maio de 2016", Bruxelas. Pp. 9 – 10. Disponível em http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+PV+20160526+SIT+DOC+PDF+V0//PT&language=PT (data da consulta: 05-12-2016).

[173] Proposta de Resolução do Parlamento Europeu, apresentada pelo Grupo Verts/ALE a 17 de Maio de 2016, sobre a transferência transatlântica de dados (2016/2727(RSP)). Disponível em http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+MOTION+B8-2016-0622+0+DOC+PDF+V0//PT (data da consulta: 05-12-2016).

[174] Resolução do Parlamento Europeu, de 26 de Maio de 2016, sobre a transferência transatlântica de dados (2016/2727(RSP)). Disponível em http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2016-0233+0+DOC+PDF+V0//PT (data da consulta: 05-12-2016).

[175] PARLAMENTO EUROPEU, "Anexo – Resultado das Votações", ponto 6, 26 de Maio de 2016. Disponível em http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+PV+20160526+RES-VOT+DOC+PDF+V0//PT&language=PT (data da consulta: 05-12-2016).

[176] PARLAMENTO EUROPEU/OBSERVATÓRIO LEGISLATIVO, "Statistics - 2016/2727(RSP) | B8-0623/2016", 26 de Maio de 2016. Disponível em http://www.europarl.europa.eu/oeil/popups/sda.do?id=27285&l=en (data da consulta: 05-12-2016).

transatlânticas, o Parlamento Europeu salientou a ideia de que uma solução duradoura para essas transferências tem necessariamente de garantir o respeito ao direito à protecção de dados e ao direito à vida privada.

Porém, e em sintonia com as preocupações expressas no parecer do Grupo de Trabalho do Art.º 29, constatou que o anexo VI do novo quadro esclarece que, de acordo com a *Presidential Policy Directive 28*, continua a ser consentida em seis casos a recolha em massa de comunicações e de dados pessoais de cidadãos não americanos. Não obstante ser salientado que essa recolha em grande escala, para ser permitida, tem que ser «tão orientada quanto possível» e «razoável», tal não satisfaz os critérios de necessidade e proporcionalidade definidos na Carta.

Na resolução, felicitou ainda os esforços da Comissão e da Administração dos EUA em obterem melhorias significativas no "Escudo de Protecção da Privacidade UE-EUA" em relação ao quadro jurídico anterior, nomeadamente com a inclusão de definições fundamentais, os mecanismos de supervisão e a obrigatoriedade de avaliações externas ou internas ao novo acordo.

Do mesmo modo, a introdução do mecanismo de recurso para os cidadãos foi classificada pelo Parlamento Europeu como positiva, ainda que tenha pedido à Comissão e à Administração dos EUA que revessem a sua complexidade, com vista a tornar o procedimento mais eficaz e fácil de usar aos cidadãos europeus.

A instituição de um mediador foi também questionada quanto à sua independência e à correspondência dos poderes que lhe são conferidos com um exercício eficaz das suas funções.

Por último, o papel de destaque dado pelo novo acordo às autoridades europeias de protecção de dados na análise e investigação das queixas atinentes à protecção de dados pessoais e na suspensão das transferências de dados, assim como a obrigação atribuída ao Departamento do Comércio de resolver essas queixas, foi outro dos aspectos tidos como positivos.

Com o intuito de influenciar a acção da Comissão, o Parlamento Europeu exortou-a a proceder a análises periódicas e aprofundadas sobre a adequação e respectivas justificações jurídicas do "Escudo de Protecção da Privacidade UE-EUA", sobretudo à luz da entrada em vigor, dentro de dois anos, do novo Regulamento.

Finalmente, o prosseguimento do diálogo com a Administração norte-americana foi considerado pelo Parlamento Europeu como essencial para negociar a correcção das deficiências apontadas no "Escudo de Protecção da Privacidade UE-EUA", pelo que insta a Comissão nesse sentido. Dando por terminada a resolução, o Parlamento Europeu encarregou o seu presidente de transmiti-la ao Conselho, à Comissão, aos governos e parlamentos dos Estados-Membros e ao governo e ao Congresso dos EUA.

5.6. Parecer da Autoridade Europeia para a Protecção de Dados

No exercício das suas competências como entidade independente de aconselhamento das instituições europeias sobre matérias relativas ao tratamento de dados pessoais[177], a AEPD emitiu um parecer sobre o "Escudo de Protecção da Privacidade UE-EUA", onde indica os aspectos críticos que encontra na proposta e as soluções que sugere.[178]

Começando por afirmar que o novo acordo não contém as salvaguardas adequadas para proteger os direitos fundamentais de protecção da privacidade e dos dados pessoais dos cidadãos europeus, a AEPD alertou para a necessidade de modificar vários pontos do "Escudo de Protecção da Privacidade UE-EUA". Recomendou, em particular, que a UE desenvolvesse garantias adicionais em termos de necessidade e proporcionalidade, ao invés de legitimar um acesso regular por parte das autoridades norte-americanas aos dados transferidos, assente em critérios jurídicos formulados na legislação dos

[177] Art. 46.º, alínea *d),* do Regulamento (CE) N.o 45/2001 do Parlamento Europeu e do Conselho de 18 de Dezembro de 2000, relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados.

[178] AUTORIDADE EUROPEIA PARA A PROTECÇÃO DE DADOS, "Opinion 4/2016 - Opinion on the EU-U.S. Privacy Shield draft adequacy decision", Bruxelas, 30 de Maio de 2016. Disponível em: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2016/16-05-30_Privacy_Shield_EN.pdf (data da consulta: 05-12-2016).

EUA, mas sem correspondência com os preceitos europeus concebidos nos Tratados e nas decisões das instituições da UE ou com as tradições constitucionais comuns entre os diferentes Estados-Membros.

Porém, a observação mais pertinente da AEPD sobre o acordo alcançado foi referente ao acesso por razões de segurança nacional aos dados transferidos: enquanto a Decisão "Porto Seguro" tratava formalmente essa hipótese como uma excepção, o "Escudo de Protecção da Privacidade UE-EUA" parece indicar, pela atenção que dedica, que o acesso e análise dos dados pessoais, transferidos para fins comerciais, por parte dos serviços de segurança norte-americanos corre o risco de se tornar uma prática frequente..

Caso tal aconteça, alertou que contrasta com as limitações a que está sujeita a UE pela legislação europeia. Esta exige que o acesso e a utilização pelas autoridades dos dados transferidos para fins comerciais, inclusive quando estejam em trânsito, só pode ocorrer em circunstâncias excepcionais e quando seja justificado por motivos específicos de interesse público. [179] Dada a exigência de que um regime de transferência transfronteiriças de dados deve assegurar um nível de protecção essencialmente equivalente ao que é garantido pelo direito da UE, essa discrepância entre os dois regimes pode ter como consequência futura a declaração de invalidade do "Escudo de Protecção da Privacidade UE-EUA". A fim de evitar isto, devem ser especificadas as finalidades para as quais se permite derrogações ao princípio da não interferência das autoridades públicas norte-americanas dos dados pessoais transferidos da UE.

Na avaliação que fez ao novo acordo, a AEPD considerou ainda que foram omissos detalhes importantes de alguns princípios de protecção da privacidade, nomeadamente em matéria de retenção de dados e tratamento automatizado, e que outras particularidades dos princípios não estão devidamente explicadas.[180] Além disso, acompanha o Grupo de Trabalho do

[179] Art. 4.º, n.º 1, alíneas *a)* a *d)*, e n.º 2 e art. 5.º, al. *a)*, do Regulamento (CE) N.o 45/2001 do Parlamento Europeu e do Conselho de 18 de Dezembro de 2000, relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados.

[180] AUTORIDADE EUROPEIA PARA A PROTECÇÃO DE DADOS, "Opinion 4/2016 - Opinion on the EU-U.S. Privacy Shield draft adequacy decision", Bruxelas, 30 de Maio de 2016. P. 7.

Art. 29 quando este afirmou que as disposições relativas às transferência subsequentes e ao exercício pelo titular do direito ao acesso e ao termo do tratamento dos dados devem ser aperfeiçoadas.

Com o intuito de melhorar os mecanismos de supervisão e reparação previstos, a AEPD sugeriu, em sintonia com o Grupo de Trabalho, que a figura do mediador fosse desenvolvida de modo a assegurar a sua independência, não só em relação aos serviços de inteligência norte-americano como também a qualquer outra autoridade.

Exortou igualmente a Comissão a procurar compromissos mais específicos de que os pedidos de informação e cooperação do mediador, bem como as suas decisões e recomendações, sejam efectivamente respeitados e implementados por todas as agências e organismos competentes. Do mesmo modo, a AEPD considerou que seria benéfica a participação de representantes da UE na apreciação dos resultados do sistema de supervisão para o tratamento, por parte das autoridades norte-americanas, dos dados pessoais transferidos da UE e na notificação de certas categorias de dados a serem tratados pelas autoridades norte-americanas, sobretudo quando esse tratamento pudesse levantar dúvidas relacionadas com os direitos fundamentais.

De acordo com as suas recomendações adicionais, aconselhou que fosse ponderada a plena integração, na decisão, dos princípios da retenção e minimização dos dados nas transferências transatlânticas para fins comerciais, visto ser essa uma forma de acautelar que o tratamento dos dados não excede o tempo necessário e é reduzido às informações pessoais que sejam relevantes para os efeitos do tratamento.

Quanto às excepções aos princípios de protecção da privacidade previstas, considerou que o âmbito dessas excepções deveria ser descrito em pormenor de forma a garantir a segurança jurídica, já que a sua amplitude pode causar dificuldade às empresas, particulares e autoridades de protecção de dados em determinar quais os tipos de tratamento de dados abrangidos por essas excepções. Além disso, algumas das excepções que estão consagradas no “Escudo de Protecção da Privacidade UE-EUA” podem ser problemáticas,

uma vez que existe a probabilidade de contradizerem requisitos fundamentais da legislação de protecção de dados da UE.

No que diz respeito à supervisão das transferências transatlânticas, a AEPD recomendou que as autoridades norte-americanas monitorizassem sistematicamente e de forma eficaz o cumprimento dos princípios, através de visitas ou inspecções às instalações das empresas auto-certificadas para determinar se esses são de facto obedecidos.

Em relação aos mecanismos de reparação dos danos provocados por uma transferência transatlântica de dados pessoais ilícita, defendeu que fosse desenvolvida a possibilidade de as empresas auto-certificadas se comprometerem a cooperar, numa base voluntária, com as autoridades nacionais de controlo[181], com vista a facilitar o acesso directo dos particulares a uma compensação pelos danos sofridos.

A este respeito, e à semelhança do que recomenda o Grupo de Trabalho do Art. 29, sustentou que as políticas de privacidade das empresas devem incluir a possibilidade de os cidadãos europeus pedirem indemnizações no espaço europeu.

Por último, a AEPD considerou ser necessária a inclusão de diversos elementos que constam no novo Regulamento, tais como os princípios da protecção de dados desde a concepção[182] e por defeito[183] e o direito à portabilidade dos dados[184].

Embora tenha saudado os esforços demonstrados pelas instituições europeias e norte-americanas em desenvolver uma solução duradoura para as transferências transatlânticas de dados que substitua a Decisão "Porto Seguro"[185], a AEPD classificou o "Escudo de Protecção da Privacidade UE-

[181] Considerando (40) do "Escudo de Protecção da Privacidade EU-EUA".
[182] Art. 25.º, n.º 1, do Regulamento Geral de Protecção de Dados.
[183] Art. 25.º, n.º 2, do Regulamento Geral de Protecção de Dados.
[184] Art. 20.º, n.º 1, do Regulamento Geral de Protecção de Dados.
[185] AUTORIDADE EUROPEIA PARA A PROTECÇÃO DE DADOS, "Opinion 4/2016 - Opinion on the EU-U.S. Privacy Shield draft adequacy decision", Bruxelas, 30 de Maio de 2016. P.12

EUA" como não sendo uma proposta sólida o suficiente para suportar um futuro escrutínio jurídico perante o TJUE.[186]

Perante este cenário, apelou que fossem feitas melhorias significativas ao novo quadro, nomeadamente no que diz respeito aos princípios da necessidade e proporcionalidade e aos mecanismos de recurso, para que esse se possa constituir como um quadro jurídico estável para as transferências de dados entre a UE e os EUA.

[186] AUTORIDADE EUROPEIA PARA A PROTECÇÃO DE DADOS, Comunicado de Imprensa "Privacy Shield: more robust and sustainable solution needed", EDPS/2016/11, 30 de Maio de 2016. Disponível em https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2016/EDPS-2016-11-PrivacyShield_EN.pdf (data da consulta: 05-01-2017).

6. REACÇÕES AO "ESCUDO DE PROTECÇÃO DA PRIVACIDADE EU-EUA"

Concebido para substituir o dispositivo precedente para a transferência transatlântica de dados pessoais, o "Escudo de Protecção da Privacidade UE-EUA" obteve, porém, críticas quanto à sua capacidade em preencher as exigências legais da UE no que diz respeito à protecção de dados pessoais e da privacidade dos cidadãos europeus. Devido a essas debilidades, muitos afirmam que a legalidade do novo acordo será facilmente questionada em sede judicial, à semelhança do que aconteceu com a Decisão "Porto Seguro".

6.1. Opiniões Favoráveis

Não obstante as dúvidas expressas por diversos organismos públicos e da sociedade civil, vários grupos representativos das empresas da indústria das tecnologias e da comunicação reagiram de forma positiva ao "Escudo de Protecção da Privacidade UE-EUA", considerando que o pacto alcançado beneficia o desenvolvimento da economia digital e das relações comerciais entre os EUA e a UE num sector cada vez mais global.

A *BSA – The Software Alliance*, que representa várias empresas internacionais de *software* com o principal objectivo de defender os direitos de propriedade industrial dos seus membros, foi uma das primeiras a manifestar o seu apoio ao "Escudo de Protecção da Privacidade UE-EUA". Num curto comunicado de imprensa, qualificou-o como estando na direcção certa para a resolução das questões mais controversas sobre a privacidade e para a manutenção da livre circulação transatlântica de dados pessoais, afirmando de imediato a total disponibilidade das empresas que fazem parte da *BSA – The Software Alliance* em auxiliar as autoridades de protecção de dados e todas as partes interessadas na transição para o novo mecanismo.[187]

Num texto dirigido ao Ministro da Segurança e Justiça holandês, a *Digital Europe* demonstrou ser favorável à adopção do "Escudo de Protecção da

[187] BSA – THE SOFTHWARE ALLIANCE, "BSA | The Software Alliance Welcomes Release of Groundbreaking Privacy Shield Text", *BSA – The Software Alliance*, Washington, 29 de Fevereiro de 2016. Disponível em http://www.bsa.org/news-and-events/news/2016/february/en02292016privacyshield?sc_lang=en (data da consulta: 05-01-2017).

Privacidade UE-EUA".[188] Na qualidade de maior associação europeia da área das tecnologias e da comunicação, esta organização alega que a invalidação da Decisão "Porto Seguro" criou um clima de incerteza jurídica que prejudica gravemente as empresas que dependem da migração de dados pessoais para a prossecução da sua actividade.

Para pôr termo a essa instabilidade jurídica, com graves consequências económicas para ambos os lados do Atlântico, a aprovação do novo quadro é por si considerada como essencial para instaurar um enquadramento legal para os fluxos transatlânticos de dados pessoais que dê garantias de protecção dos direitos fundamentais aos cidadãos europeus e de estabilidade às empresas, após a declaração de invalidade do mecanismo precedente. Nesse sentido, remete para um estudo jurídico, desenvolvido pela *Hogan Lovells*, que expõe diversos argumentos que sustentam a tese de que o novo acordo atende aos critérios estabelecidos no Acórdão Schrems.[189]

Embora encare o pacto alcançado como sendo mais exigente para as empresas, por impor, por exemplo, a celebração de um contrato para a transferência ulterior de dados entre parceiros comerciais, a *Digital Europe* exorta a que se prossiga a uma rápida adopção do "Escudo de Protecção da Privacidade UE-EUA", dado crer que este incluiu as salvaguardas necessários para assegurar um nível elevado de protecção dos dados pessoais, ao mesmo tempo que possibilita às empresas do sector das tecnologias e da comunicação a expansão dos seus negócios, num momento em que a transferência transfronteiriça de dado possui um papel fulcral na economia global.

A *Microsoft*, uma das maiores empresas da indústria tecnológica, anunciou publicamente o seu apoio ao novo mecanismo, comprometendo-se de imediato a assiná-lo ainda antes de ser aprovado. Dando seguimento ao que tinha declarado, tornou-se na primeira provedora de serviços em nuvem

[188] HIGGINS, John, "RE: Future Adoption of the draft EU-US Privacy Shield Adequacy Decision (Article 31 Committee)", *Digital Europe,* Bruxelas, 11 de Abril de 2016. Disponível em http://www.digitaleurope.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&EntryId=2151&PortalId=0&TabId=353 (data da consulta: 05-12-2016).

[189] USTARAN, Eduardo *et al*, "Legal Analysis of the EU-U.S. Privacy Shield: An adequacy assessment by reference to the jurisprudence of the Court of the Justice of the European Union"", *Hogan Lovells*, 31 de Março de 2016. Disponível em http://www.hoganlovells.com/files/Uploads/Documents/Privacy%20Shield%20Legal%20Analysis%20by%20Hogan%20Lovells%20(2016-03-31).pdf (data da consulta: 05-12-2016).

("*cloud*") a aparecer na lista do Departamento do Comércio das entidades certificadas para transferir dados pessoais ao abrigo do novo quadro.[190]

Numa declaração publicada no *blog* da companhia, o vice-presidente para assuntos governamentais na UE afirmou que o pacto alcançado constitui uma base sólida e eficaz para a circulação de dados entre os EUA e a UE por estabelecer meios de protecção da privacidade mais fortes e pragmáticos para os cidadãos europeus, enquanto permite o movimento contínuo de dados. [191]

A exigência de transparência dos pedidos governamentais de acesso a informações pessoais, assim como a de delimitação dos casos em que esse acesso é autorizado, e a criação de abordagens alternativas aos particulares para a resolução de disputas no domínio da utilização dos seus dados pessoais são outros dos factores mencionados pela *Microsoft* para justificar a sua posição favorável relativamente à aprovação do acordo tal como foi negociado.

A *Computer & Communications Industry Association* (CCIA), cuja principal missão é a de promover os interesses legítimos das empresas que actuam nas áreas das tecnologias da informação, da informática e das telecomunicações, também considerou benéfica a adopção do novo quadro.

Nas palavras do director da CCIA Europa, o novo quadro estabelece um padrão elevado para as transferências transatlânticas, constituindo, por isso, uma vitória para a protecção da privacidade dos particulares e para as empresas, já que poderão contar com regras mais claras e precisas sobre o modo como os fluxos de dados se devem operar no âmbito do "Escudo de Protecção da Privacidade UE-EUA". [192]

---

[190] RISON, Alice, "Microsoft Cloud is first CSP behind the Privacy Shield", *Microsoft Azure,* 26 de Setembro de 2016. Disponível em https://azure.microsoft.com/pt-pt/blog/microsoft-cloud-is-first-csp-behind-the-privacy-shield/ (data da consulta: 05-01-2017).

[191] FRANK, Jonh, "Microsoft's commitments, including DPA cooperation, under the EU-U.S. Privacy Shield", *Microsoft*, 11 de Abril de 2016. Disponível em https://blogs.microsoft.com/eupolicy/2016/04/11/microsofts-commitments-including-dpa-cooperation-under-the-eu-u-s-privacy-shield/ (data da consulta: 05-01-2017).

[192] GREENFIELD, Heather, "Privacy Shield Adopted: Clarity For Firms, Privacy Win For Consumers", *CCIA,* 12 de Julho de 2016. Disponível em http://www.ccianet.org/2016/07/privacy-shield-adopted-clarity-for-firms-privacy-win-for-consumers/ (data da consulta: 05-01-2017).

Posição semelhante é assumida ainda pela *Information Technology Industry Council* (ITI), uma associação comercial que representa as empresas do sector de tecnologia da informação e das comunicações e que, em um comunicado de imprensa, expressou o seu apoio pelos mesmos motivos. [193]

6.2. Opiniões Desfavoráveis

O "Escudo de Protecção da Privacidade UE-EUA" teve uma recepção negativa junto de vários organismos públicos e da sociedade civil, que o classificaram de insatisfatório por não proteger devidamente os dados pessoais dos cidadãos europeus de futuras ingerências por parte das autoridades norte-americanas.[194]

Schrems, o activista responsável pelo processo que levou à revogação do anterior quadro transatlântico para as transferências de dados pessoais, tornou-se numa das vozes mais críticas quanto a uma possível aprovação do "Escudo de Protecção da Privacidade UE-EUA". Embora admita que o acordo alcançado traga algumas melhorias em relação ao mecanismo precedente, alega que nenhum desses avanços se reporta a preocupações com as falhas das leis de vigilância dos EUA e a ausência de leis de protecção de privacidade no direito norte-americano, tornando-o vulnerável a futuros processos judiciais.[195]

Para sustentar a sua posição, citou uma carta do *Office of the Director of National Intelligence*, que consiste no anexo VI do "Escudo de Protecção da Privacidade UE-EUA", em que se afirma que os dados pessoais obtidos em massa podem ser utilizados para seis fins específicos.

Ao prever explicitamente esses seis casos excepcionais, o novo acordo está a contrariar as indicações do TJUE, dadas no Acórdão Schrems, de que qualquer programa de vigilância indiscriminada em larga escala baseado no

[193] INFORMATION TECHNOLOGY INDUSTRY COUNCIL, "ITI Praises EU-US Privacy Shield Approval by European Governments", *Information Technology Industry Council*, Washington, 8 de Julho de 2016. Disponível em http://www.itic.org/news-events/news-releases/iti-praises-eu-us-privacy-shield-approval-by-european-governments (data da consulta: 05-01-2017).
[194] Acórdão Schrems §93 e 94.
[195] EUROPE VERSUS FACEBOOK, "Privacy Shield – Press Breakfast by MEP Jan Albrecht", *Europe versus Facebook,* Bruxelas, 12 de Julho de 2016. Disponível em http://www.europe-v-facebook.org/PA_PS.pdf (data da consulta: 05-01-2017).

acesso a dados pessoais viola a lei europeia, por comprometer a essência do direito fundamental ao respeito pela vida privada e pela intimidade. Contesta, portanto, a Comissão quando esta assevera que os EUA comprometeram-se a não permitir aos serviços nacionais de segurança que efectuassem programas de vigilância indiscriminada de grande dimensão.

No prosseguimento das suas críticas ao conteúdo do pacto alcançado, Schrems considerou igualmente que o mesmo não teve em consideração a exigência do TJUE de que um novo quadro para as transferências transatlânticas de dados deverá fornecer uma "equivalência essencial" ao que seja assegurado pelo direito comunitário em matéria de protecção de dados pessoais. Como justificação, referiu o facto de não ser abordada a questão da utilização indevida de dados pessoais pelo sector privado, distanciando, neste ponto, das regras fundamentais sobre o uso de dados pelos privados que estão consagradas no direito da UE.

Adicionalmente, Schrems sugeriu noutro texto que o art. 3.º da decisão de execução do novo acordo, referente à obrigação do Estado-Membro em informar a Comissão quando a autoridade nacional competente suspende ou proíbe a transferência de dados para uma empresa norte-americana, mesmo que esta seja subscritora dos princípios de privacidade previstos, é passível de criar instabilidade jurídica para aquelas que adoptaram esses princípios. Dito de outro modo, ao não existir nenhuma garantia legal de que os fluxos de dados irão sucessivamente ocorrer por terem aderido ao novo quadro transatlântico, as empresas signatárias correm o risco de serem prejudicadas por uma decisão da autoridade de protecção de dados do Estado-Membro em causa, dado estas poderem determinar a suspensão ou proibição da transferência de dados para uma empresa sediada nos EUA. [196]

Pelas falhas que aponta ao novo acordo, acredita que o "Escudo de Protecção da Privacidade UE-EUA" está condenado ao fracasso por não constituir uma solução estável para os cidadãos europeus e para as empresas,

[196] SCHREMS, Maximillian, ""EU-US Privacy Shield": Towards a new Schrems 2.0 Case?", *European Area of Freedom Security & Justice*, São Francisco, 3 de Abril de 2016. Disponível em https://free-group.eu/2016/04/06/eu-us-privacy-shield-towards-a-new-schrems-2-0-case/ (data da consulta: 05-01-2017).

sendo que a maioria destas irá rejeitá-lo como principal base jurídica para as transferências transatlânticas de dados devido a essas limitações. Além disso, antevê ainda que diversos particulares irão contestar judicialmente o novo acordo, por sofrer dos mesmos vícios que levaram à revogação da Decisão "Porto Seguro".[197]

Tal como o activista austríaco, foram várias as organizações não-governamentais (doravante, «ONGs») que se opuseram à adopção do "Escudo de Protecção da Privacidade UE-EUA" como quadro jurídico para os fluxos transatlânticos de dados pessoais.

Numa carta dirigida aos presidentes do Grupo de Trabalho do Art. 29.º e da Comissão das Liberdades Cívicas, da Justiça e dos Assuntos Internos e ao embaixador e representante permanente da Holanda junta da UE, mais de vinte ONGs pediram que fossem retomadas as negociações em torno do "Escudo de Protecção da Privacidade UE-EUA", uma vez que este, tal como se encontra, não obedece aos critérios estabelecidos pelo TJUE no Acórdão Schrems e não protege adequadamente os dados pessoais dos cidadãos europeus. Entre aquelas que subscreveram a carta constam, entre outras, a *Electronic Privacy Information Center* (EPIC), a *Digital Rights Ireland* e a *La Quadrature du Net.* [198]

Para que o novo acordo pudesse constituir-se como uma estrutura viável a longo prazo para as transferências transatlânticas de informações pessoais, as ONGs afirmaram igualmente que seria necessário, entre outras medidas, que os EUA procedessem a uma reforma legislativa em matéria de protecção de dados, dado que as actuais leis em vigor estão longe de assegurar um nível de protecção essencialmente equivalente àquele que vigora no espaço europeu.

Apesar dos esforços, o "Escudo de Protecção da Privacidade UE-EUA" acabou por ser adoptado pela Comissão a 12 de Julho de 2016. Em função

[197] LOMAS, Natasha, "Draft Text Of EU-U.S. Privacy Shield Deal Fails To Impress The Man Who Slayed Safe Harbor", *TechCruch*, 29 de Fevereiro de 2016. Disponível em https://techcrunch.com/2016/02/29/lipstick-on-a-pig/ (data da consulta: 05-01-2017).

[198] ELECTRONIC PRIVACY INFORMATION CENTER (EPIC), "NGOs - "Privacy Shield" is Failed Approach for EU-US Data Protection", *EPIC*, 16 de Março de 2016. Disponível em https://epic.org/2016/03/ngos---privacy-shield-is-faile.html (data da consulta: 05-01-2017).

disso, duas das ONGs que assinaram a carta – a *Digital Rights Ireland*[199] e a *La Quadrature du Net*[200] – interpuseram no TJUE recursos de anulação a solicitarem que seja anulada a decisão da Comissão que aprovou o novo quadro, esperando, assim, cessar a vigência de um mecanismo que consideram inadequado para salvaguardar os direitos dos cidadãos europeus quando os seus dados são transferidos para os EUA.

6.3. Síntese Conclusiva

Concebido para ser um acordo sólido que assegurasse a continuidade da livre circulação de dados entre a UE e os EUA, os responsáveis pelo "Escudo de Protecção da Privacidade UE-EUA" afirmaram que a avaliação realizada à adequação do nível de protecção garantido pelas leis norte-americanas obedeceu aos critérios traçados pelo TJUE no Acórdão Schrems. Idênticos aos que estão previstos no art. 45.º, n.º 2, do Regulamento, os elementos que a Comissão deve ter em consideração quando adopta uma decisão de adequação são os seguintes:

- Existência de normas na legislação do país terceiro que limitem possíveis ingerências nos direitos fundamentais dos titulares dos dados transferidos à estrita medida do necessário, inclusive quando sejam invocadas razões de segurança nacional ou de interesse público;
- Impedimento do acesso generalizado aos dados pessoais transferidos por parte das autoridades públicas do país terceiro, o que implica a existência legal de um critério objectivo que delimite o acesso e posterior uso dos dados pelas autoridades estatais a fins que sejam estritamente susceptíveis de justificar essa ingerência;

[199] Recurso de Anulação interposto pela *Digital Rights Ireland* contra a Comissão no Tribunal de Justiça da União Europeia, de 16 de Setembro de 2016, do processo T-670/16. Disponível em http://curia.europa.eu/juris/document/document.jsf?text=&docid=185146&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=244203 (data da consulta: 05-01-2017).

[200] Recurso de Anulação interposto pela *La Quadrature du Net* contra a Comissão no Tribunal de Justiça da União Europeia, de 10 de Outubro de 2016, do processo T-738/16. Informações retiradas em http://curia.europa.eu/juris/fiche.jsf?id=T%3B738%3B16%3BRD%3B1%3BP%3B1%3BT2016%2F0738%2FP (data da consulta: 05-01-2017).

- Atribuição de garantias de acesso, rectificação e supressão dos dados pessoais aos cidadãos europeus, em virtude da legislação interna ou dos compromissos internacionais assumidos pelo país terceiro.
- Confirmação de que o país terceiro assegura uma protecção aos dados pessoais substancialmente equivalente à que vigora no espaço europeu, ainda que os meios utilizados para tal sejam distintos.

No entanto, se analisarmos o anexo VI do novo acordo, deparamos com a previsão explícita de seis casos excepcionais em que é permitido às autoridades norte-americanas acederem aos dados dos cidadãos europeus para fins distintos daqueles que justificaram originalmente a sua transferência.

Com base nessas excepções, é possível admitir a hipótese de uma recolha maciça e indiscriminada de dados provenientes da UE por parte dos serviços de segurança norte-americanos, o que vai contra a exigência, expressa no Acórdão Schrems, de que qualquer acesso das autoridades públicas aos dados transferidos tem que ser proporcional ao estritamente necessário para a obtenção do fim pretendido, de forma a garantir que os direitos fundamentais de respeito pela intimidade e de protecção de dados pessoais dos cidadãos europeus não são infringidos.

A figura do mediador, celebrada por constituir um novo mecanismo de recuso disponível aos titulares europeus de dados que queiram reivindicar os seus direitos contra acções ilícitas dos serviços de segurança norte-americanos, cria incertezas quanto à sua independência, uma vez que será desempenhada por um alto membro do Departamento do Comércio. A imparcialidade que se exige ao mediador no desempenho das suas funções pode, assim, ficar comprometida.

A extensão dos poderes que o mediador dispõe para responder às queixas que recebe é também questionável. De acordo com o que consta no anexo III, secção 4, al. *e)*, a resposta do mediador às pretensões do particular limitar-se-á a confirmar que a queixa foi *"devidamente investigada"* e que os textos legais referentes às limitações e garantias aplicáveis foram respeitados ou, em caso

de incumprimento, que este foi emendado. Daqui resulta, tal como é dito, que o autor da reclamação nunca será informado pelo mediador se foi ou não alvo de vigilância e qual a reparação específica aplicada, não existindo hipótese de recurso. Ao impossibilitar que quem recorra a este mecanismo fique a conhecer os verdadeiros contornos do caso que denuncia e a solução encontrada, limita-se de forma drástica a capacidade de o mediador se constituir como o intermediário dos cidadãos europeus junto das autoridades públicas norte-americanas.

Perante a análise sucinta que se fez, conclui-se que vários aspectos relevantes do "Escudo de Protecção da Privacidade UE-EUA" não seguem devidamente os critérios estabelecidos no Acórdão Schrems, ao contrário daquilo que tinha sido prometido pela Comissão e pela Administração norte-americana.

Tal como sucedeu com a Decisão "Porto Seguro", as diferenças materiais entre as ordens jurídicas dos EUA e da UE dificultam a construção de um quadro jurídico para as transferências transatlânticas de dados. O facto de a lei norte-americana não reconhecer a protecção de dados pessoais como um direito fundamental, o que redunda na inexistência de um regime legal com critérios rígidos para a recolha, utilização e retenção de dados para fins comerciais, são alguns dos aspectos que contrastam fortemente com aquilo que é norma no direito da União.

Além disso, os EUA não aderiram à Convenção 108 do Conselho da Europa e ao seu Protocolo Adicional respeitante às autoridades de controlo e aos fluxos transfronteiriços de dados, sendo que ambos estão abertos à adesão de Estados não-europeus e foram assinados pela totalidade dos Estados-Membros da UE.

Neste contexto, torna-se difícil aos EUA apresentarem garantias de que asseguram um nível de protecção de dados equivalente ao que existe na UE, um dos requisitos imprescindíveis para que seja tomada a decisão de autorizar a circulação regular de dados pessoais para um país terceiro.

Esta visão sobre as fragilidades do novo acordo é, aliás, corroborada pelos pareceres do Grupo de Trabalho do Art.º 29 e da AEPD, bem como pela resolução, de 26 de Maio de 2016, do Parlamento Europeu. Schrems, o responsável pelo desencadear do processo que levou à cessação da vigência da Decisão "Porto Seguro", também formulou críticas semelhantes às que constam nos textos dos referidos órgãos europeus, o que demonstra uma certa homogeneidade na recepção ao novo quadro legal. Por concordamos com a sua fundamentação, consideramos que procedem as críticas negativas ao "Escudo de Protecção da Privacidade UE-EUA".

7. CONCLUSÕES

Partindo da análise ao Acórdão Schrems, que declarou a invalidade da Decisão "Porto Seguro", procurou-se desenvolver, ao longo da presente tese, um estudo em que fossem abordadas as principais dificuldades que se colocam ao estabelecimento de um quadro legal que permita o livre fluxo de dados pessoais da UE para as empresas norte-americanas, num momento em que tais transferências assumem um papel crucial na economia transatlântica e as preocupações com o eventual acesso das autoridades públicas aos dados transferidos são crescentes.

Após um longo período de negociações, os EUA e a UE acordaram um novo enquadramento legal para as transferências transatlânticas de dados pessoais, destinado a preencher o espaço deixado vago pelo mecanismo precedente: o "Escudo de Protecção da Privacidade UE-EUA".

No entanto, apesar dos esforços em conceder um quadro jurídico que reflectisse as exigências enunciadas no Acórdão Schrems, o quadro acordado recebeu fortes críticas por manter as mesmas fraquezas que levaram à invalidação da Decisão "Porto Seguro", o que denota a complexidade em definir uma regulamentação que concilie os interesses económicos dos dois lados do Atlântico com a protecção adequada dos dados pessoais e da privacidade dos cidadãos europeus. Em geral, os comentários desfavoráveis ao novo acordo devem-se à manutenção do acesso das autoridades públicas norte-americanas aos dados pessoais em casos específicos, à fragilidade dos novos meios de recurso quanto à sua independência e competência e às divergências entre os níveis de protecção assegurados pelos EUA e pela UE.

Neste capítulo, em função das conclusões obtidas com a investigação efectuada ao longo do trabalho, somos capazes de dar uma resposta àquela que estabelecemos como a questão de investigação da presente tese: *será que se pode qualificar o "Escudo de Protecção da Privacidade UE-EUA" como um quadro jurídico viável para as transferências transatlânticas de dados pessoais, tendo em conta os critérios estabelecidos pelo TJUE no Acórdão Schrems e as críticas que recebeu?*

Dada a verificação de vários elementos relevantes do novo acordo que não estão conformes com as exigências do TJUE no Acórdão Schrems, o "Escudo de Protecção da Privacidade UE-EUA" terá dificuldade em ser considerado um quadro jurídico estável e duradouro para as relações comerciais entre os EUA e a UE, uma vez que não constitui uma regulamentação sólida o suficiente para suportar um futuro escrutínio jurídico perante o TJUE.

Caso o TJUE proceda à avaliação dos aspectos mais frágeis do "Escudo de Protecção da Privacidade UE-EUA", a possibilidade de este ter o mesmo destino que a Decisão "Porto Seguro" é elevada. A declaração de invalidade do novo acordo poderá ter sérias consequências:

- Primeira, para as empresas que necessitam da livre circulação de dados pessoais para o prosseguimento e desenvolvimento da sua actividade, o que redundará igualmente no enfraquecimento da economia digital e das relações comerciais transatlânticas;
- Segunda, para a credibilidade das autoridades norte-americanas e europeias, com especial destaque para as da UE, num momento em que cresce o cepticismo em torno do projecto europeu, como comprovam o *Brexit* e a crescente popularidade dos partidos anti-europeístas em diversos Estados-Membros;
- Terceira, para a própria ideia da existência de um mecanismo legal que permita a livre transferência de dados pessoais da UE para as empresas norte-americanas sem que os direitos fundamentais dos cidadãos europeus sejam afectados, já que será a segunda vez que um acordo com esse propósito será considerado inválido. A crença em conseguir um pacto que garanta uma protecção dos dados transferidos para os EUA considerada substancialmente equivalente à que é assegurada pela legislação europeia ficará, assim, abalada.

Não obstante reconhecer-se o impacto que terá a anulação do novo acordo, o certo é que a vulnerabilidade do "Escudo de Protecção da Privacidade UE-EUA" deve-se a falhas estruturais que não podem ser resolvidas casuisticamente, uma vez que têm origem nas diferentes percepções sobre a protecção de dados pessoais entre o direito norte-americano e o europeu.

Contrariamente ao que sucede na UE, nos EUA não é reconhecido um direito fundamental à protecção de dados pessoais. A legislação norte-americana sobre esta matéria é altamente fragmentada, divergindo consoante o sector, tipo de dados e Estado que esteja em causa. Em resultado, a auto-regulação das empresas é incentivada quando essas procedam à recolha e tratamento de dados pessoais.

Devido às características que lhe são inerentes, o regime norte-americano não fornece um nível de protecção de dados pessoais que se possa considerar como adequado e equivalente ao assegurado na UE, precisamente o critério a observar pela Comissão quando adopta uma decisão a consentir as transferências de dados para um país terceiro.

Em função das razões expostas, consideramos que a Comissão não deveria ter aprovado o "Escudo de Protecção da Privacidade UE-EUA", visto não serem dadas garantias suficientes de que os direitos fundamentais dos cidadãos europeus em matéria de privacidade e protecção de dados continuarão a ser respeitados após os seus dados serem transferidos para os EUA. Além disso, em caso de ingerência das autoridades norte-americanas nos dados pessoais que lhe digam respeito, não existe nenhum mecanismo de recurso indiscutivelmente independente ao dispor do particular, já que, em relação ao mediador, existem dúvidas fundadas quanto à sua parcialidade e às suas competências.

No "Escudo de Protecção da Privacidade UE-EUA" estão previstas reapreciações anuais e conjuntas da Comissão e do Departamento do Comércio, para avaliarem se as conclusões relativas à adequação do nível de protecção garantido pelos EUA se mantêm factual e legalmente justificadas. Porém, tais reapreciações partem do pressuposto de que os EUA já asseguram um nível adequado de protecção de dados, o que não acontece. Assim, embora estas reavaliações periódicas possam ser utilizadas para corrigir alguns dos aspectos mais frágeis do novo acordo, não poderão, por si só, resolver as diferenças irreconciliáveis entre as ordens jurídicas norte-americanas e europeias, que somente poderão ser dissipadas com uma profunda reforma legislativa dos EUA em matéria de protecção de dados

Devido às fragilidades apontadas, é expectável que a vigência do "Escudo de Protecção da Privacidade UE-EUA" seja de curta duração, sobretudo quando duas organizações não-governamentais já apresentaram no TJUE recursos de anulação a solicitarem que seja declarada a invalidade do novo acordo.[201] Nesta perspectiva, as negociações para um novo quadro para as transferências transatlânticas de dados pessoais só deverão ser iniciadas caso os EUA se comprometam a reformular as suas leis e assinar as mais relevantes convenções internacionais sobre a protecção de dados, a fim de conseguirem garantir um nível de protecção equivalente ao que vigora na UE.

Na era digital em que vivemos, as transferências de dados pessoais assumem cada vez mais um papel de destaque na economia internacional, pelo que são compreensíveis os esforços dos Estados em celebrarem acordos que facilitem a existência desses fluxos de dados. Porém, tal não deve levar a UE a abdicar da protecção dos dados pessoais e do respeito pela intimidade dos cidadãos dos diferentes Estados-Membros em prol dos benefícios económicos obtidos pelos fluxos transfronteiriços de dados, uma vez que esses são princípios elevados à categoria de direitos fundamentais na legislação europeia por serem considerados essenciais para a liberdade e livre expressão dos cidadãos europeus.

[201] Recursos de anulação interpostos pela *Digital Rights Ireland*, a 16 de Setembro de 2016, do processo T-670/16, e pela *La Quadrature du Net*, a 10 de Outubro de 2016, do processo T-738/16.

8. BIBLIOGRAFIA

Monografias e capítulos de livros:

- AGÊNCIA DOS DIREITOS FUNDAMENTAIS DA UNIÃO EUROPEIA, CONSELHO DA EUROPA, *Manual da Legislação Europeia sobre Proteção de Dados*, Serviço das Publicações da União Europeia, Luxemburgo, 2014. Disponível em http://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-pt.pdf (data da consulta: 05-12-2016)
- CASTRO, Catarina Sarmento e, *Direito da Informática, Privacidade e Dados Pessoais*, Almedina, 2005.
- FARINHO, Domingos Soares, *Intimidade da Vida Privada e Media no Ciberespaço*, Almedina, 2006.
- CAMPOS, João Luiz Mota de, CAMPOS, João Mota de, *Manual de Direito Europeu - O sistema institucional, a ordem jurídica e o ordenamento económico da União Europeia,´*7.ª edição, Coimbra Editora, 2010.
- LOPES, J. de Seabra, "A Protecção da Privacidade e dos Dados Pessoais na Sociedade da Informação: tendências e desafios numa sociedade em transição", in *Estudos dedicados ao Prof. Doutor Mário Júlio de Almeida Costa*, Universidade Católica Editora, 2002.

Artigos de Revistas Jurídicas:

- ALVAREZ, Daniel, "Safe Harbor is dead; Long Live the Privacy Shield?" in *Business Law Today,* n. º 5, Maio de 2016. Pp. 1 – 5.
- ARAÚJO, Alexandra Maria Rodrigues, OLIVEIRA, José Sebastião de, "A Transferência de dados pessoais para países terceiros acompanhada de uma decisão de adequação no direito da União Europeia" in *Direito e Novas Tecnologias (XXIII Congresso Nacional do Conpedi/UFPB: A Humanização*

do Direito e a Horizontalização da Justiça no Século XXI), 2015. Pp. 282 – 308.

- DORT, Kenneth K., CRISS, Jennifer T., "Trends in Cybersecurity Law, the Privacy Shield, and Best Practices for Businesses Operating in the Global Marketplace" in *The Computer & Internet Lawyer*, vol. 33, n.º 7, Julho de 2016. Pp. 5 – 10.
- FARINHO, Domingos Soares, "(Un)Safe Harbour: Comentário à Decisão do TJUE C-362/14 e suas Consequências Legais", in *Fórum de Proteção de Dados,* n.º 2, Janeiro de 2016. Pp. 109 – 124.
- HOWELL, Chanley, KALYVAS, James, RIDLEY, Eileen, TANTLEFF, Aaron, LIGNIER, Sophie, MILLENDORF, Steven, MITRO, Elizabeth, "EU-U.S. Privacy Shield Agreement Released" in *Journal of Health Care Compliance*, Maio e Junho de 2016. Pp. 19 – 66.
- JAEGER, Jaclyn, "EU-U.S. Privacy Shield passes: Now what?" in *Compliance Week*, Setembro de 2016. Pp. 46 – 48.
- LOIDEAN, Nora Ni, "The End of Safe Harbor: Implications for EU Digital Privacy and Data Protection Law" in *Journal of Internet Law,* vol. 19, n.º 8, Fevereiro de 2016. Pp. 1 e 8 – 14.
- RAMALHO, David Silva, COIMBRA, José Duarte, "A declaração de invalidade da Diretiva 2006/24/CE: presente e futuro da regulação sobre conservação de dados de tráfego para fins de investigação, deteção e repressão de crimes graves" in *O Direito*, Coimbra, Ano 147.º – IV, 2015. Pp. 997 – 1046.
- VOSS, W. Gregory, "The Future of Transatlantic Data Flows: Privacy Shield or Bust?" in *Journal of Internet Law,* vol. 19, n.º 11, Maio de 2016. Pp. 1 e 9 – 18.

Artigos e Notícias consultados *online*:

- CHAFREY, Dave, "Global social media research summary 2016", *Smart Insights*, 8 de Agosto de 2016. Disponível em http://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research/ (data da consulta: 05-12-2016).
- CAROLAN, Mary, "US government wants to be joined in Schrems case", *The Irish Times*, 13 de Junho de 2016. Disponível em http://www.irishtimes.com/business/technology/us-government-wants-to-be-joined-in-schrems-case-1.2683066 (data da consulta:05-12-2016).
- CAROLAN, Mary, "Ruling against data transfer regime may cost Europe €143bn a year, says Facebook", *The Irish Times*, 7 de Julho de 2016. Disponível em http://www.irishtimes.com/business/technology/ruling-against-data-transfer-regime-may-cost-europe-143bn-a-year-says-facebook-1.2713685 (data da consulta: 05-12-2016).
- CAROLAN, Mary, "Schrems and Facebook privacy case: next round set for February", *The Irish Times*, 25 de Julho de 2016. Disponível em http://www.irishtimes.com/business/technology/schrems-and-facebook-privacy-case-next-round-set-for-february-1.2733961 (data da consulta: 05-12-2016).
- DOWNES, Larry, "The Business Implications of the EU-U.S. "Privacy Shield" , *Harvard Business Review*, 10 de Fevereiro de 2016. Disponível em https://hbr.org/2016/02/the-business-implications-of-the-eu-u-s-privacy-shield (data da consulta: 05-12-2016).
- GIBBS, Samuel e agências, "Max Schrems Facebook privacy complaint to be investigated in Ireland", *The Guardian*, 20 de Outubro de 2015. Disponível em https://www.theguardian.com/technology/2015/oct/20/max-

schrems-facebook-privacy-ireland-investigation (data da consulta: 05-12-2016).

- GUERRA, Ana Rita, "Europa e EUA chegam a acordo para substituir 'Safe Harbour', *BIT Magazine,* 3 de Fevereiro de 2016. Disponível em http://www.bit.pt/europa-e-eua-chegam-a-acordo-para-substituir-safe-harbour/ (data da consulta: 05-12-2016).
- HILL, Kashmir (2016), "Max Schrems: The Austrian Thorn In Facebook's Side", *Forbes*, 7 de Fevereiro. Disponível em http://www.forbes.com/sites/kashmirhill/2012/02/07/the-austrian-thorn-in-facebooks-side/#3b30af996b30 (data da consulta: 05-12-2016).
- KELLENHER, Denis, "The next four legal steps for the Privacy Shield", *International Association of Privacy Professionals (IAPP)*, 16 de Fevereiro de 2016. Disponível em https://iapp.org/news/a/the-next-four-steps-for-the-privacy-shield/ (data da consulta: 05-12-2016).
- LESLIE, Andre, "Facebook viola os direitos fundamentais na Europa, diz activista", *Deutsche Welle (DW),* 10 de Julho de 2013. Disponível em http://dw.com/p/194dR (data da consulta: 05-12-2016).
- LOMAS, Natasha, "Draft Text Of EU-U.S. Privacy Shield Deal Fails To Impress The Man Who Slayed Safe Harbor", *TechCrunch,* 29 de Fevereiro de 2016. Disponível em https://techcrunch.com/2016/02/29/lipstick-on-a-pig/ (data da consulta: 05-12-2016).
- MIÑO, Veronica, "European Data Protection Supervisor about the Privacy Shield", *datenschutz notizen,* 13 de Junho de 2016. Disponível em https://www.datenschutz-notizen.de/european-data-protection-supervisor-about-the-privacy-shield-2814895/ (data da consulta: 05-12-2016).
- PROTALINSKI, Emil, "Facebook: Releasing your personal data reveals our trade secrets", *ZD Net*, 12 de Outubro de

2011. Disponível em http://www.zdnet.com/article/facebook-releasing-your-personal-data-reveals-our-trade-secrets/ (data da consulta: 05-12-2016).

- PRIVACY LAWS & BUSINESS, "Ireland to challenge model clauses as basis for international transfers", *Privacy Laws & Business*, 26 de Maio de 2016. Disponível em https://www.privacylaws.com/Publications/enews/International-E-news/Dates/2016/5/Ireland-to-challenge-model-clauses-as-basis-for-international-transfers/ (data da consulta: 05-12-2016).
- RTÉ NEWS, "Commercial Court hears US government arguments for involvement in data protection case", *RTÉ News*, 7 de Julho de 2016. Disponível em http://www.rte.ie/news/2016/0707/800815-facebook-data-commissioner/ (data da consulta: 05-12-2016).
- STUPP, Catherine, "EU privacy watchdogs demand improvements to 'Privacy Shield'", *EurActiv,* 13 de Abril de 2016. Disponível em http://www.euractiv.com/section/digital/news/eu-privacy-watchdogs-demand-improvements-to-privacy-shield/ (data da consulta: 05-12-2016).

Outros Textos:

- EUROPE VERSUS FACEBOOK, "Legal Procedure against "Facebook Ireland Limited". Disponível em http://europe-v-facebook.org/EN/Complaints/complaints.html (data da consulta: 05-12-2016).
- EUROPE VERSUS FACEBOOK, "Rapid Press Update: Facebook & NSA-Surveillance: Following "Safe Harbor" decision, Irish Data Protection Commissioner to bring EU-US data flows before CJEU again", *Europe versus Facebook*, 25 de Maio de 2016, 2.ª versão. Disponível em http://www.europe-v-facebook.org/PA_MCs.pdf (data da consulta: 05-12-2016).

- EUROPE VERSUS FACEBOOK, "Rapid Press Update: Facebook & NSA-Surveillance: Following "Safe Harbor" decision, Irish Data Protection Commissioner to bring EU-US data flows before CJEU again", *Europe versus Facebook*, 25 de Maio de 2016, 2.ª versão. Disponível em http://www.europe-v-facebook.org/PA_MCs.pdf (data da consulta: 05-12-2016).
- EUROPE VERSUS FACEBOOK, "US government joins Facebook EU-US data transfer case as "amicus"", *Europe versus Facebook*, 19 de Julho de 2016. Disponível em http://www.europe-v-facebook.org/PA_AJ.pdf (data da consulta: 05-12-2016.
- HIGGINS, John, "RE: Future Adoption of the draft EU-US Privacy Shield Adequacy Decision (Article 31 Committee)", *Digital Europe*, Bruxelas, 11 de Abril de 2016. Disponível em http://www.digitaleurope.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&EntryId=2151&PortalId=0&TabId=353 (data da consulta: 05-12-2016).
- SCHREMS, Maximilian, "Complaint against Facebook Ireland Ltd – 23 "PRISM"", Viena, 25 de Junho de 2013. Disponível em http://www.europe-v-facebook.org/prism/facebook.pdf (data da consulta: 05-12-2016).
- SCHREMS, Maximilian, "Complaint against Facebook Ireland Ltd", Viena, 1 de Dezembro de 2015. Disponível em http://www.europe-v-facebook.org/comp_fb_ie.pdf (data da consulta: 05-12-2016).

Índice