Algumas considerações sobre a compatibilidade do sistema de *Privacy Shield* com o direito da União Europeia à luz do acórdão Schrems

Martinho Lucas Pires*

Resumo: O presente artigo tem por objeto a análise crítica dos principais elementos do sistema de *Privacy Shield*, relativo à transferência de dados entre a União Europeia e os Estados Unidos da América. A análise parte dos critérios normativos de direito da União Europeia que devem rodear a apreciação do nível de proteção de dados garantido por um país terceiro, estabelecidos pelo Tribunal de Justiça da União Europeia no acórdão *Schrems*. Tais considerações demonstram que importantes características do *Privacy Shield* suscitam sérias dúvidas de legalidade, colocando em dúvida o futuro de tal sistema a médio e longo prazo.

Palavras-chave: *Direito da União Europeia; Proteção de Dados; Direitos Fundamentais; Relações UE-EUA.*

Abstract: The purpose of this article is to critically analyse the main elements of the Privacy Shield framework on the transfer of data between the European Union and the United States of America. In order to do so, this article shall start from an assessment of the framework in light of the normative criteria of European Union law as set out by the Court of Justice of the European Union in the *Schrems* case. This analysis shows that important characteristics of *Privacy Shield* raise serious questions of legality that cast a shadow over the long-term feature of the framework.

Keywords: *European Union Law; Data Protection; Fundamental rights; Relations EU-USA.*

---

* Licenciado e mestre em Direito pela Faculdade de Direito da Universidade Católica Portuguesa. Doutorando em direito da União Europeia pela Faculdade de Direito da Universidade Nova de Lisboa. Bolseiro da Fundação para a Ciência e Tecnologia. Advogado, com inscrição suspensa por motivos académicos. Assistente convidado da Faculdade de Direito da Universidade Católica Portuguesa. Escreve sobre os temas de Direito Constitucional, Direito da União Europeia, Direito Económico e Protecção de Dados. Este artigo foi escrito com o apoio de uma bolsa da Fundação para a Ciência e Tecnologia.

Introdução

O quadro normativo sobre a recolha, armazenamento, tratamento e transferências de dados pessoais na UE tem sido alvo de grandes e profundas transformações nos últimos anos[1]. Deve-se este facto ao grande desenvolvimento que entretanto se verificou no campo das chamadas tecnologias de informação[2]. A utilização e subscrição de serviços comerciais, de entretenimento, e dos mais variados tipos, através de mecanismos digitais que são facilmente acessíveis através de instrumentos portáteis como um telefone ou um simples relógio tornou-se tão comum que é hoje um comportamento normal e recorrente. Não só da vivência cultural e social mas, sobretudo, económica. Basta um "clique" numa tecla ou um "toque" num ecrã para que uma série de informações possa ser transmitida para um outro aparelho, que pode estar localizado num território não só *distinto* como também bastante *distante* do lugar onde o utilizador se encontra. Esta facilidade de comunicação levou a um aumento exponencial de transferências territoriais de dados, possibilitando o desenvolvimento de vários negócios dedicados somente à economia digital, naquilo que se diz ser o primeiro mercado, pela sua natureza e características, naturalmente global[3].

Esta digitalização de serviços económicos trouxe consigo vários desafios de regulação, tendo em conta a vulnerabilidade a que os mesmos dados estão sujeitos. De facto, os dados não são só facilmente transmissíveis; são igualmente objeto de fácil recolha ou tratamento por parte de entidades privadas (empresas, associações) quer por entidades públicas (administração fiscal ou policial). Tratamento esse que pode ou não ser indevido, se

---

[1] Para uma análise histórica da evolução sobre legislação de protecção de dados na UE, v. Agência dos Direitos Fundamentais da União Europeia e Conselho da Europa "Handbook on European data protection law", 2014. Disponível em: <http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf> (acedido a 25/10/2017).

[2] V. igualmente, sobre esta evolução e evolução das regulações comerciais, o artigo de Andrade de Jesus, Inês Oliveira. "O direito à proteção de dados pessoais e o regime jurídico das transferências internacionais de dados: a proteção viaja com as informações que nos dizem respeito?", publicado no presente Anuário.

[3] Sobre o impacto económico das transferências internacionais de dados, v. Conferência das Nações Unidas sobre Comércio e Desenvolvimento, "Data protection regulations and international data flows: Implications for trade and development", 2016. Disponível em: <http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf> (acedido a 25/10/2017).

não for conhecido e autorizado de antemão pelo utilizador. Cabe assim às autoridades políticas estabelecer sistemas de normas e meios práticos que permitam uma proteção eficaz dos direitos de privacidade dos titulares destes dados – sem no entanto afetar em demasia a liberdade de transmissão dos mesmos num mundo global.

Esta fácil mobilidade de dados entre diferentes ordens jurídicas é um dos problemas mais importantes desta nova realidade digital. Isto porque, no caso da UE, muitas das grandes empresas que operam (e, de certa forma, têm uma posição determinante) no seu mercado interno são oriundas dos EUA, como a *Apple*, *Google*, *Facebook*, *Amazon*, entre outras. A estrutura multinacional destas empresas, com certos serviços internos divididos entre vários territórios e continentes, faz com que os dados dos consumidores e utilizadores (e, igualmente, dos trabalhadores) destas empresas sejam passíveis de tratamento em vários locais, com regimes jurídicos diversos. Consequentemente, os utilizadores estarão sujeitos a diferentes níveis de proteção dos seus direitos à privacidade e à intimidade da vida privada, dependendo da ordem jurídica em que se encontrem os seus dados. Coloca-se, deste modo, o desafio de estabelecer mecanismos jurídicos que possam garantir a efetiva proteção de dados a um nível razoavelmente semelhante ao gozado pelos utilizadores no seu território residencial, quando tais dados são transmitidos para territórios terceiros.

O sistema atualmente em vigor quanto à transferência de dados pessoais de cidadãos europeus para empresas sediadas nos EUA é denominado de *Privacy Shield* ou "Escudo de Proteção". Este sistema foi considerado adequado face às normas europeias de proteção de dados pela Decisão de Execução da Comissão número 2016/1250, de 12 de julho de 2016 (doravante "Decisão *Privacy Shield*"). O *Privacy Shield* veio substituir os princípios de *Safe Harbor* que se encontravam em vigor desde há dezassete anos[4], e que em 2015 foram considerados incompatíveis com o direito da União Europeia pelo Tribunal de Justiça no acórdão *Schrems*[5]. O conteúdo desta sentença judicial acabou por afetar a elaboração da Decisão de *Privacy*

[4] Comissão Europeia, Decisão 2000/520 EC com fundamento na Diretiva 95/46/CE do Parlamento Europeu e do Conselho relativa ao nível de proteção assegurado pelos princípios de Porto Seguro e Resposta a Questões pelo Departamento de Estado dos EUA, de 26 de julho de 2000.

[5] Acórdão do TJ, C-362/14, *Maximilian Schrems* v. *High Authority*, de 6 de outubro de 2015.

Shield, ao estabelecer de forma contundente critérios normativos que limitam a ação da Comissão ao apreciar a adequação de um sistema jurídico de proteção de direitos de titulares de dados pessoais de um país terceiro com o sistema da UE. Apesar da aprovação de uma decisão de adequação, subsistem ainda sérias dúvidas sobre a compatibilidade do *Privacy Shield* com as normas do direito da UE sobre proteção de dados pessoais. Estas dúvidas foram expressas por autoridades públicas de proteção de dados europeias e nacionais[6] e por órgãos políticos como o Parlamento Europeu[7].

O propósito deste artigo é apresentar algumas considerações relativas quanto ao juízo de compatibilidade do *Privacy Shield* com as normas de direito da UE sobre a transmissão e a proteção de direitos dos titulares de dados pessoais para um país terceiro. Para tal efeito iremos, numa primeira parte, ver quais os requisitos normativos da UE relativos à transmissão de dados para países terceiros. Iremos analisar não só as normas em vigor mas sobretudo a interpretação que lhes foi dada pelo Tribunal de Justiça no acórdão *Schrems*. Em seguida, numa segunda parte, faremos uma breve descrição da Decisão de *Privacy Shield* e de quais os seus traços gerais em termos de forma, estrutura e conteúdo. Na terceira parte olharemos de forma crítica para a Decisão de *Privacy Shield*, tendo por base não só a sua compatibilidade com os requisitos normativos em causa face a certos preceitos analisados em abstrato, mas também considerando a questão da sua aplicação prática por parte das autoridades públicas norte-americanas. Terminaremos com uma breve consideração sobre o futuro do sistema de *Privacy Shield* e das transferências de dados transatlânticas.

---

[6] Autoridade Europeia para a Protecção de Dados, "Opinion 4/2016 on the EU-U.S. Privacy Shield draft adequacy decision", de 30 de maio de 2016. Disponível em: <https://edps.europa.eu/sites/edp/files/publication/16-05-30_privacy_shield_en.pdf> (acedido a 25/10/2017); e G29, "Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decision", adoptada a 13 de abril de 2016. Disponível em: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf> (acedido a 25/10/2017).

[7] Parlamento Europeu, Proposta de Resolução Comum de 24 de maio de 2016. Disponível em: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+MOTION+P8-RC-2016-0623+0+DOC+PDF+V0//EN> (acedido a 25/10/2017); e Parlamento Europeu, Proposta de Resolução de 29 de março de 2017. Disponível em: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+MOTION+B8-2017-0235+0+DOC+PDF+V0//PT> (acedido a 25/10/2017).

2. Requisitos normativos para transferências de dados da UE para países terceiros

2.1. Requisitos legislativos: Diretiva 95/46/CE

O regime de transferência de dados da UE para países terceiros encontra-se regulado no capítulo IV da Diretiva 95/46/CE do Conselho e do Parlamento (doravante a "Directiva"), mais concretamente nos art. 25.º e 26.º. Dispõe o n.º 1 do primeiro art. que as transferências de dados pessoais para países terceiros só podem ser realizadas caso o país em questão – país recetor – assegure um nível de proteção adequado para os dados, ou caso alguma das exceções estabelecidas na Diretiva ocorra. Quer isto dizer que a transferência de dados da UE para países terceiros é em princípio *proibida* caso não estejam preenchidas as condições previstas na Diretiva.

A averiguação da adequação do nível de proteção de dados do país recetor deverá ser efetuada, de acordo com o n.º 2 do art. 25.º, "em função de todas as circunstâncias que rodeiem a transferência ou o conjunto de transferências de dados". Para o efeito desta avaliação, deve ter-se em conta uma série de critérios, tais como: a natureza dos dados, a razão de ser do tratamento e sua duração, o local de origem dos dados para tratamento e o local de destino após tratamento, o regime jurídico de proteção de dados no país terceiro, e "as regras profissionais e as medidas de segurança" que são respeitadas no território do país recetor. Cabe à Comissão, nos termos do disposto no n.º 6 do mesmo art., após averiguação do preenchimento destes critérios, tomar uma decisão, declarando se o país terceiro oferece ou não um nível de proteção adequada de tratamento de dados pessoais, tendo em conta a respetiva legislação nacional e compromissos internacionais assumidos por esse país recetor.

Como foi mencionado *supra* existem exceções a este regime, estabelecidas nas alíneas a) a f) do art. 26.º n.º 1. A transferência pode ser efetuada independentemente do país terceiro oferecer ou não um nível de proteção adequada nos seguintes casos: se uma pessoa dado o seu consentimento inequívoco à transferência de dados; se a transferência efetuada a partir de um registo público; se a transferência necessária para a celebração de um contrato e efetuada no interesse do titular dos dados, ou se for efetuada para proteger um interesse público, ou para exercer um direito de defesa num processo judicial, ou ainda para proteger os interesses vitais do titular

dos dados. Importa também referir que, nos termos do art. 26.º n.º 2, caso um Estado-Membro ou a Comissão considerem que existem, em concreto, cláusulas contratuais que garantam direitos de proteção da vida privada e condições de exercício desses respetivos direitos, a transferência de dados para um país terceiro que não ofereça um nível de proteção adequado é permitida.

A Diretiva foi recentemente revogada pelo RGPD. Este diploma passará a ser aplicável a partir de 18 de maio de 2018, segundo o seu art. 99.º, pelo que cabe verificar o quadro normativo relativo às transferências de dados para países terceiros[8].

A matéria sobre transferência de dados para países terceiros encontra-se disposta no capítulo V do Regulamento, nos arts. 44.º a 50.º. O nível de regulação é mais desenvolvido do que na Diretiva. A regra geral continua a ser a de que a transferência de dados é proibida a não ser que exista uma decisão de adequação da Comissão que considere o nível de proteção de dados pessoais do país terceiro como sendo adequado. Contudo, o art. 45.º n.º 1 alíneas a) a c) apresenta uma lista reforçada de critérios para avaliação da adequação. Aos critérios do art. 25.º n.º 1 da Diretiva acrescentam-se: a existência do "primado do Estado de Direito, o respeito pelos direitos humanos e liberdades fundamentais"; a aplicação e respeito de regras de proteção de dados, nas quais se incluem as que são desenvolvidas por jurisprudência; a existência de "direitos dos titulares dos dados efetivos e oponíveis, e vias de recurso administrativo e judicial para os titulares de dados cujos dados pessoais sejam objeto de transferência"; e "a existência e o efetivo funcionamento de uma ou mais autoridades de controlo independentes no país terceiro ou às quais esteja sujeita uma organização internacional" com capacidade coerciva. Deve ter-se igualmente em conta o facto do país recetor estar ou não sob a alçada de instrumentos jurídicos internacionais de carácter vinculativo sobre esta matéria.

Caso não exista uma decisão de adequação, os responsáveis de tratamento de dados só podem transferi-los desde que apresentem garantias adequadas de proteção e que os titulares dos dados disponham de direitos e mecanismos judiciais de reação que sejam eficazes, nos termos do

---

[8] Cabe dizer neste ponto que a elaboração do quadro normativo do Regulamento, em particular quanto aos critérios necessários que a decisão de adequação deve preencher, foi bastante influenciado pelas considerações que o TJ fez no acórdão *Schrems*, como se verificará após a análise do *douto aresto*.

art. 46.º n.º 1. Estas garantias adequadas, nos termos do n.º 2, podem ser previstas através de instrumentos jurídicos vinculativos "e com força executiva entre autoridades ou organismos públicos", regras vinculativas de autoridades nacionais de controlo[9], cláusulas-tipo de proteção de dados adotadas ou aprovadas pela Comissão, códigos de conduta emitidos ao abrigo do art. 40.º ou procedimentos de certificação ao abrigo do art. 42.º. Quanto às derrogações, o regime do art. 49.º transcreve, na prática, o regime do n.º 1 do art. 26.º da Diretiva, acrescentando-se no entanto que, caso uma transferência não tenha por base uma decisão de adequação nem preencha as derrogações dos art. 46.º ou do n.º 1 do art. 49.º, só pode ocorrer se:

> (...) não for repetitiva, apenas disser respeito a um número limitado de titulares dos dados, for necessária para efeitos dos interesses legítimos visados pelo responsável pelo seu tratamento, desde que a tais interesses não se sobreponham os interesses ou os direitos e liberdades do titular dos dados, e o responsável pelo tratamento tiver ponderado todas as circunstâncias relativas à transferência de dados e, com base nessa avaliação, tiver apresentado garantias adequadas no que respeita à proteção de dados pessoais.

Por fim, o art. 50.º do Regulamento estabelece que a Comissão e as autoridades nacionais de controlo devem prosseguir com esforços contínuos de cooperação internacional no domínio de proteção de dados[10].

2.2. Interpretação dos requisitos normativos: o caso Schrems

Como decorre da exposição anterior, a questão principal quanto ao critério para permitir a transferência de dados de forma generalizada

---

[9] Ao abrigo do art. 47.º do Regulamento, as autoridades de controlo podem emitir regras vinculativas relativas ao tratamento e às transferências de dados por empresas ou grupos de empresas. Essas regras devem especificar, nos termos das várias alíneas do n.º 2 do artigo, uma série de elementos, entre os quais os direitos dos titulares e métodos de reação e exercício desses mesmos direitos, bem como procedimentos internos de supervisão do tratamento e de reclamação sobre o mesmo.

[10] Sobre as transferências de dados ao abrigo do Regulamento, v. Andrade de Jesus, Inês Oliveira. "O direito à proteção de dados pessoais e o regime jurídico das transferências internacionais de dados: a proteção viaja com as informações que nos dizem respeito?", publicado no presente Anuário.

prende-se com o entendimento que deve ser dado à expressão "nível de proteção adequado". Existem critérios de averiguação amplos, mas não existe uma definição exata do conceito de adequação. Neste sentido, caberia à Comissão, no âmbito dos poderes que lhe foram atribuídos pela Diretiva, realizar tal juízo dentro dos seus poderes discricionários.

A questão foi discutida no acórdão *Schrems* pelo TJ. O caso em questão tem por base a ação intentada por um cidadão austríaco, Maximilian Schrems, contra o *Data Protection Commissioner*, a autoridade de controlo de proteção de dados da Irlanda. Após as revelações de Edward Snowden – antigo funcionário da NSA, uma agência de segurança e investigação pertencente à administração dos EUA – a vários órgãos de comunicação social internacionais sobre as práticas de vigilância operadas pelos serviços secretos dos EUA, que recolhiam de forma generalizada e indiscriminada dados pessoais armazenados em sistemas de comunicação diversos através da NSA, Schrems fez uma queixa ao *Data Protection Commissioner.* A queixa assentava no facto de a rede social Facebook, da qual Schrems era utilizador, transferir dados de clientes para os EUA, onde poderiam ser alvo de recolha por parte dos serviços secretos norte-americanos. Deste modo, Schrems requeria que as autoridades irlandesas deixassem de autorizar a transferência de dados e investigasse se o Facebook permitia ou não a recolha dos mesmos por parte das autoridades norte-americanas. A autoridade de controlo irlandesa recusou-se a ouvir a queixa por considerar que esta carecia de fundamento, e remeteu para a existência da decisão da Comissão que considerava que o nível de proteção existente nos EUA, assente nos princípios de *Safe Harbor,* era adequado.

Insatisfeito com a decisão, Schrems recorreu judicialmente para a *High Court,* o Supremo Tribunal irlandês. Este órgão jurisdicional, ao contrário do *Data Protection Commissioner,* considerou que os efeitos das revelações Snowden não podiam ser ignorados, e que existiam dúvidas sobre se a decisão de adequação da Comissão face ao sistema de *Safe Harbor* era ou não válida ao abrigo da CDFUE[11]. No entanto, cabia saber se a decisão de adequação impedia ou não as autoridades nacionais de controlo de prosseguir uma queixa individual que lhes fosse colocada, havendo suspeitas de risco de utilização indevida de dados. O Supremo Tribunal Irlandês

[11] Acórdão do TJ, C-362/14, ECLI:EU:C:2015:650, *Schrems*, paras. 30 a 35, de 6 de outubro de 2015.

decidiu questionar o TJ, através do mecanismo de reenvio prejudicial, relativamente ao grau de vinculação que o art. 25.º n.º 1 da Diretiva impõe à autoridade nacional de proteção de dados relativamente à decisão de adequação da Comissão[12].

O TJ tratou prontamente de responder a esta questão, considerando que ao abrigo da Diretiva e da interpretação que lhe deve ser dada segundo os art. 7.º – respeito pela vida privada e familiar – e 8.º – proteção de dados pessoais – da CDFUE, a autoridade nacional de proteção de dados pode investigar queixas relativas ao tratamento de dados em países terceiros, mesmo se existir já uma decisão de adequação prévia[13]. Entender o contrário seria retirar os poderes às autoridades nacionais de proteção de dados e limitar o direito dos particulares a uma proteção judicial efetiva, nos termos do art. 47.º da Carta.

Em seguida, em vez de dar o caso por terminado, o tribunal europeu decidiu debruçar-se sobre a decisão de adequação *per se*. Ou seja, o TJ quis olhar para a validade da decisão face às normas europeias sobre transferências de dados. Para tal, era necessário interpretar o significado de nível proteção adequado à luz dos artigos da CDFUE mencionados *supra*, e no seguimento da recente jurisprudência do TJ consagrada à interpretação destas normas no ordenamento jurídico da UE, mormente no acórdão *Digital Rights*[14].

---

[12] *Idem*, para. 36.

[13] "Atendendo às considerações anteriores, há que responder às questões submetidas que o artigo 25.º, n.º 6, da Diretiva 95/46, lido à luz dos artigos 7.º, 8.º e 47.º da Carta, deve ser interpretado no sentido de que uma decisão adotada ao abrigo desta disposição, como a Decisão 2000/520, através da qual a Comissão constata que um país terceiro assegura um nível de proteção adequado, não obsta a que uma autoridade de controlo de um Estado-Membro, na aceção do artigo 28.º desta diretiva, examine o pedido de uma pessoa relativo à proteção dos seus direitos e liberdades em relação ao tratamento de dados pessoais que lhe dizem respeito que foram transferidos de um Estado-Membro para esse país terceiro, quando essa pessoa alega que o direito e as práticas em vigor neste último não asseguram um nível de proteção adequado". Acórdão do TJ, C-362/14, ECLI:EU:C:2015:650, *Schrems*, para. 66, de 6 de outubro de 2015.

[14] Acórdão do TJ, C-293/12 e C-594/12, *Digital Rights Ireland*, de 8 de abril de 2014, sobre uma análise do caso, v. Granger, Marie-Pierre e Irion, Kristina. "The Court of Justice and the Data Retention Directive in Digital Rights Ireland: Telling Off the EU Legislator and Teaching a Lesson in Privacy and Data Protection", *European Law Review*, vol. 39, n.º 6, 2014, pp. 835-850 e Ramalho, David e Coimbra, José Eduardo. "A declaração de invalidade da

Neste sentido, o TJ afirmou que por nível de proteção adequado deve entender-se que o quadro de proteção de direitos dos titulares de dados do país terceiro é "substancialmente equivalente" ao que é oferecido pela UE[15]. Isto não significa que um país terceiro tenha de ter um sistema exatamente *idêntico* ao da UE mas sim, nas palavras do TJ, que este país deve dispor de meios jurídicos "efetivos, na prática" para proteção dos direitos dos titulares, "para assegurar uma proteção substancialmente equivalente à garantida dentro da União[16]". Apesar de reconhecer o poder de apreciação da Comissão, o TJ alega que este é limitado, dados os requisitos estipulados pelo art. 25.º da Diretiva e os direitos estabelecidos na CDFUE. Deve, portanto, ser aplicado e fiscalizado de forma estrita[17].

O TJ trata então de identificar três características essenciais que o sistema de proteção de direitos dos titulares de dados do país terceiro deve garantir para ser considerado equivalente ao da UE. A primeira característica é a *eficácia* do próprio sistema. A Comissão deve averiguar se os instrumentos jurídicos de proteção dos direitos do respeito pela vida privada e do tratamento de dados em vigor no país terceiro são capazes, na prática, de detetar, responsabilizar e punir de forma completa e real quaisquer infrações aos seus preceitos[18]. Em segundo lugar, só são permitidas interferências na esfera jurídica de proteção dos direitos fundamentais constantes dos art. 7.º e 8.º da CDFUE *de forma excecional*, ou seja, quando tiverem por fim a prossecução de um objetivo de interesse geral ou comum; quando estiverem definidas por regras claras e precisas; quando estabelecerem exigências mínimas de garantias de tratamento de dados; e, por fim, quando forem efetuadas na estreita medida do necessário e segundo um critério de proporcionalidade,

---

Diretiva 2006/24/CE: presente e futuro da regulação sobre conservação de dados de tráfego para fins de investigação, deteçãoo e repressão de crimes graves", *O Direito*, Ano 147.º, IV, 2015, pp. 997-1046.

[15] TJ, C-362/14, ECLI:EU:C:2015:650, *Maximilian*, para.73, de 6 de outubro de 2015.

[16] *Idem*, para. 74.

[17] *Idem*, para. 78 sobre a discricionariedade da Comissão e do seu papel na fundamentação do critério de adequação, v. o artigo de Rodrigues de Oliveira, Ricardo. "'What's in a name? Uma breve análise do nível de proteção adequado no âmbito das transferências de dados pessoais dos cidadãos da UE para países terceiros" publicado no presente Anuário.

[18] TJ, C-362/14, ECLI:EU:C:2015:650, *Maximilian*, para.73, de 6 de outubro de 2015, para. 81.

tal como preconizado anteriormente no acórdão *Digital Rights*[19]. Por fim, a Comissão deve averiguar se existem meios de recurso judicial ao dispor do titular dos dados que lhe garantam *uma forma de reação efetiva* contra as empresas de tratamento. Como afirma o TJ, "uma regulamentação que não preveja nenhuma possibilidade de o particular recorrer a vias de direito para ter acesso aos dados pessoais que lhe dizem respeito, ou para obter a retificação ou a supressão de tais dados, não respeita o conteúdo essencial do direito fundamental a uma proteção jurisdicional efetiva, tal como é consagrado no art. 47.º [da CDFUE][20]".

Após ter desenvolvido estes três pontos o TJ passou à análise do sistema norte-americano de *Safe Harbor*. O tribunal não colocou, em abstrato, entraves ao facto deste quadro regulatório assentar num regime de auto-certificação[21]. No entanto, considerou que existiam dúvidas sobre a sua fiabilidade pelo facto dos princípios não se aplicarem às autoridades públicas norte-americanas[22] e da decisão da Comissão não apresentar "constatações suficientes" sobre a adequação do nível de proteção garantido pelo ordenamento jurídico norte-americano[23]. Em segundo lugar, o TJ entendeu que a "Decisão 2000/520 consagra o primado dos "requisitos de segurança nacional, interesse público ou [cumprimento da lei]", sendo que sempre que haja uma lei norte-americana sobre matéria de segurança que regule em sentido contrário aos princípios de *Safe Harbor* as empresas de tratamento devem obedecer-lhe em detrimento dos princípios[24]. Esta supremacia do

---

[19] *Idem*, para 91.

[20] *Idem*, para 95.

[21] *Idem*, para 81 quer isto dizer que o sistema norte-americano é baseado numa série de princípios que as empresas de tratamento de dados escolhem adotar e implementar por si mesmos e cujo compromisso é posteriormente comunicado a uma autoridade pública, de modo a poder beneficiar da liberdade transferência de dados ao abrigo. Sobre o sistema de proteção de dados norte-americano, v. Cole, David e Fabbrini, Federico. "Bridging the Transatlantic Divide? The United States, the European Union, and the Protection of Privacy Across Borders", *iCourts Working Paper Series*, n.º 33, 2015, pp. 1-19; e Hasty, Robert; Nagel, Trevor W. e Subjally, Mariam. "Data Protection Law in the U.S.A", *Advocates for International Development,* 2013. Disponível em: <https://www.neighborhoodindicators.org/sites/default/files/course-materials/A4ID_DataProtectionLaw%20.pdf> (acedido a 25/10/2017).

[22] Acórdão do TJ, C-362/14, ECLI:EU:C:2015:650, *Schrems*, para. 82, de 6 de outubro de 2015.

[23] *Idem*, para. 83.

[24] *Idem*, paras. 84 e 85.

princípio de segurança nacional face à proteção dos direitos fundamentais dos particulares é, na opinião do TJ, excessiva e desequilibrada, pois a decisão de adequação não apresenta "qualquer referência à existência, nos Estados Unidos, de normas de caráter estatal destinadas a limitar as eventuais ingerências nos direitos fundamentais das pessoas cujos dados pessoais sejam transferidos da União para os Estados Unidos, ingerências essas que as autoridades estatais deste país seriam autorizadas a praticar quando prosseguem objetivos legítimos, tais como a segurança nacional[25]". Assim, existe o risco de as interferências, em vez de serem a exceção, poderem ser a regra. O facto de a regulamentação norte-americana autorizar não só a conservação da totalidade dos dados pessoais de forma indiscriminada e arbitrária[26] mas também o acesso de modo generalizado ao conteúdo de comunicações electrónicas[27] faz com que o TJ considere que não é respeitado o princípio de que as ingerências à esfera de proteção dos direitos fundamentais só podem operar na "estrita medida do necessário". Por fim, o tribunal entende que não existem mecanismos administrativos ou judiciais que permitam ao particular aceder aos seus dados e pedir a sua retificação ou supressão, o que viola o direito a uma tutela jurisdicional efetiva estabelecido no art. 47.º da CDFUE[28].

Em suma, o TJ conclui que a Comissão não apresentou de forma fundamentada informações de que os EUA, nos termos do art. 25.º n.º 6 da Diretiva, dispõem de um sistema de regulação que garanta um nível adequado e substancialmente equivalente ao nível que existe na UE. O tribunal não considera necessário olhar em concreto para o conteúdo dos princípios de *Safe Harbor,* visto que o art. 1.º da decisão de adequação não cumpre com os requisitos estabelecidos na Diretiva, interpretados à luz dos direitos fundamentais estabelecidos nos art. 7.º, 8.º e 47.º da CDFUE. Assim, o TJ considerou que o art. 1.º da decisão de adequação é inválido[29]. Finalmente, após análise crítica do art. 3.º da mesma decisão e da invalidade dos limites aí estabelecidos aos poderes das autoridades nacionais para conhecer

[25] *Idem*, para. 88.
[26] *Idem*, para. 93.
[27] *Idem*, para. 94.
[28] *Idem*, para. 95.
[29] *Idem*, para. 98.

de queixas particulares, o TJ acabou por declarar que toda a decisão era inválida face ao ordenamento jurídico da UE[30].

3. Os Princípios de *Privacy Shield*

3.1. Breve história dos princípios de Privacy Shield

Ao anular a decisão de adequação sobre os princípios de *Safe Harbor*, o TJ tornou mais premente a conclusão de um processo que se encontrava em marcha à data do acórdão *Schrems*.

Em 2013 a Comissão Europeia emitiu um comunicado anunciando as suas dúvidas face à efetividade do *Safe Harbor*[31]. Para a Comissão tornava-se necessário reexaminar o sistema não só à luz das alterações contextuais que se verificaram entretanto na sociedade económica, com o "aumento exponencial dos fluxos de dados" e sua importância no desenvolvimento do comércio digital e transatlântico, mas também face às questões sobre o "nível da proteção" efetivamente garantido[32]. As autoridades nacionais dos Estados-Membros da UE notavam que a adesão aos princípios não era muito seguida na práctica, e de que existiam dúvidas sobre qual o verdadeiro grau de interferência de entidades públicas dos EUA, como a NSA, na recolha e tratamento indiscriminado de dados por empresas americanas[33]. A Comissão identificou igualmente problemas na supervisão e aplicação coerciva dos princípios de *Safe Harbor* por parte dos reguladores americanos[34].

---

[30] *Idem*, paras. 105 e 106. Para uma visão mais abrangente das consequências do caso, v. Ojanen, Thomas. "Rights-Based Review of Electronic Surveillance after Digital Rights Ireland and Schrems in the European Union", *in*: David Cole *et al.* (ed.). *Surveillance, Privacy and Transatlantic Relations* Oxford: Hart Publishing, 2017, pp. 13-30.

[31] Comissão Europeia, "Comunicação da Comissão ao Parlamento Europeu e ao Conselho sobre o funcionamento do sistema 'porto seguro' na perspetiva dos cidadãos da UE e das empresas estabelecidas na UE", de 27 de novembro de 2013. Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52013DC0847&qid=1488287495250&from=PT> (acedido a 25/10/2017). Cabe dizer igualmente que muitos elementos desta comunicação são citados pelo TJ no acórdão *Schrems*.

[32] Comissão Europeia, "Comunicação...", cit, p. 3.

[33] *Idem*, pp. 5-8.

[34] *Idem*, pp. 11-15.

No fundo, a Comissão constatou que existiam graves deficiências práticas no sistema de *Safe Harbor* que permitiam o acesso indiscriminado e arbitrário a dados de cidadãos europeus por parte de autoridades americanas. Constatou-se ainda que as vias de recurso ao dispor dos titulares dos dados para contestar qualquer interferência abusiva contra os seus direitos eram limitadas[35]. A Comissão verificou igualmente que havia problemas de transparência quanto à utilização de derrogações aos princípios de Safe Harbor por parte de empresas americanas[36]. O órgão executivo máximo da UE concluiu deste modo que "o acesso em grande escala pelos serviços de informações a dados transferidos para os EUA por empresas certificadas participantes no sistema de 'porto seguro' levanta novas questões graves sobre a continuidade dos direitos dos cidadãos europeus em matéria de proteção de dados quando os seus dados pessoais são transferidos para os EUA[37]".

Perante este cenário a Comissão apresentou várias recomendações[38]. Primeiro, deve-se melhorar a transparência do sistema, ou seja, a exigência de publicação e comunicação por parte de empresas aderentes de todas as políticas de proteção de dados que têm em vigor e seu cumprimento efetivo com os princípios de proteção em vigor. Em segundo lugar, deve-se trabalhar a questão dos meios de reação judicial disponíveis. Entende-se por este ponto que deve procurar-se a instituição de um sistema mais acessível, menos oneroso e mais fiável ao dispor dos particulares para recorrer a mecanismos de resolução de litígios, quer sejam mecanismos de resolução alternativa de litígios ou outras formas. Em terceiro lugar, é necessário que haja maior aplicação de controlos regulatórios por parte das autoridades americanas, em particular quanto à supervisão efetiva de queixas dos particulares face a empresas que não cumpram com os princípios de proteção de dados em vigor. Por fim, e em quarto lugar, o acesso a dados por parte das autoridades norte-americanas ao abrigo das exceções acordadas como o princípio de segurança nacional só pode e deve ser efetuado de forma que respeite critérios de necessidade e proporcionalidade face ao respeito dos direitos de privacidade dos particulares.

---

[35] *Idem*, pp. 18 e 19.

[36] *Idem*, pp. 19 e 20.

[37] *Idem*, p. 20.

[38] *Idem*, pp. 20-22.

Iniciou-se posteriormente a esta comunicação um processo de melhoramento do *Safe Harbor* efetuado em conjunto pelas autoridades americanas e europeias. As negociações tiveram início em 2014, sendo aceleradas a partir de 2015 devido ao acórdão *Schrems*[39]. Apesar da urgência em atingir um acordo, dada à situação de incerteza provocada pela falta de uma decisão (incerteza que afetava negativamente todo o mercado económico de base digital e seus agentes), o processo enfrentou várias dificuldades. Chegou-se a pensar que as discussões poderiam estar irremediavelmente votadas ao fracasso[40]. No entanto, em fevereiro de 2016 a Comissão conseguiu apresentar um projeto de decisão de adequação, tendo por base a existência de um novo sistema para as empresas americanas, chamado *Privacy Shield*. Após consideração das opiniões do G29 onde se reúnem representantes das autoridades de controlo dos Estados-Membros, e da AEPD, a Comissão aprovou a nova decisão de adequação, que foi publicada a 1 de agosto de 2016, dez meses após o acórdão *Schrems*.

3.2. Forma, estrutura e conteúdo do Privacy Shield

O *Privacy Shield*, tal como o *Safe Harbo*r, é um sistema norte-americano de proteção de dados transferidos da UE para os Estados Unidos. A apresentação do sistema e dos seus princípios é acompanhada por uma série de declarações de entidades públicas norte-americanas. Quanto à decisão de adequação, é um ato normativo da UE, de carácter geral mas não legislativo, tomada pela Comissão ao abrigo de uma delegação de poderes consagrada no art. 25.º n.º 6 da Diretiva, permitida pelo art. 290.º TFUE.

A estrutura da Decisão *Privacy Shield* é semelhante à da decisão de adequação do *Safe Harbor.* A decisão contém uma lista de considerandos que versam sobre o contexto, descrição e justificação do ato jurídico, seguido

---

[39] Comissão Europeia, "Decisão de execução da Comissão número 2016/1250, relativa ao nível de proteção assegurado pelo Escudo de Proteção da Privacidade UE-EUA, com fundamento na Diretiva 95/46/CE do Parlamento Europeu e do Conselho", de 12 de julho de 2016, p. 3.

[40] Voss, Gregory W. "The Future of Transatlantic Data Flows: Privacy Shield or Bust", *Journal of Internet Law*, vol. 19, n.º 11, 2016, p. 11.

do conteúdo normativo da decisão *per se*, e de uma lista de anexos. O que difere a Decisão *Privacy Shield* da decisão de adequação do *Safe Harbor* neste aspeto estrutural é a sua extensão[41]. Justifica-se esta maior dimensão com duas situações provocadas pelo acórdão *Schrems*. A primeira tem que ver com a obrigação da Comissão justificar *fundadamente* a adequação do sistema. O TJ foi contundente no acórdão a estabelecer critérios normativos detalhados a que a Comissão deve obedecer para poder decidir se um sistema jurídico de um país terceiro garante ou não um nível de proteção substancialmente equivalente ao da UE. Em segundo lugar, era necessário que os EUA apresentassem maiores garantias, não só do ponto de vista regulatório (nível *micro* de proteção, *vis-à-vis* as empresas), mas também (e em particular) do ponto de vista dos poderes das autoridades nacionais de investigação e segurança (nível *macro* de proteção, *vis-à-vis* o Estado).

Quanto ao conteúdo, as grandes diferenças entre os princípios de *Privacy Shield* e os princípios de *Safe Harbor* verificam-se no maior desenvolvimento e precisão das normas e do aumento das obrigações para as empresas, de garantias de supervisão e de meios de recursos para os cidadãos europeus. O *Privacy Shield* procura assim não só responder às dúvidas da Comissão face as aparentes deficiências do *Safe Harbor*, mas também às críticas do TJ no acórdão *Schrems*, intenção declarada de forma explícita nos considerandos 4 a 13 da decisão.

Mantêm-se o sistema de autocertificação, pelo que cabe às empresas americanas apresentar às entidades reguladoras (DOC e FTC) a sua adesão aos princípios e o cumprimento efetivo dos mesmos. Mantêm-se igualmente os princípios do *Safe Harbor* – a saber: aviso, escolha, responsabilização pela transferência ulterior, segurança, integridade dos dados e limitação dos objetivos, acesso e recurso, aplicação e responsabilidade – embora mais trabalhados e desenvolvidos quanto ao alcance das obrigações para as empresas[42]. Destacam-se igualmente a existência de novas obrigações de informação das empresas perante os titulares de dados, relativamente não só às políticas de recolha e de tratamento, mas também aos meios de

---

[41] A decisão de adequação do *Safe Harbor* tinha 47 páginas, com 11 considerandos, 4 artigos e 7 anexos. A Decisão *Privacy Shield*, por seu turno, tem 112 páginas, com 155 considerandos, 6 artigos e 7 anexos.

[42] Comissão Europeia, "Decisão de execução...", Anexo II, pp. 48-52.

reação internos (dentro da estrutura da empresa) e externos (recurso a meios de resolução alternativa) que os particulares dispõem para poder aceder ou reagir contra o tratamento a que os seus dados estão sujeitos. Foi adicionada igualmente uma lista de princípios suplementares que estabelece novas obrigações e que complementam e consolidam os sete princípios iniciais[43], como por exemplo ao nível de proteção do tratamento de dados que se deve verificar em grupos de empresas, ou quanto à proteção a ter relativamente a situações sectoriais específicas (dados relativos a informação médica, laboral, jornalística, etc).

Destacam-se igualmente novos mecanismos de recurso, podendo o particular escolher reagir diretamente perante a empresa, uma autoridade de controlo nacional ou um organismo independente de resolução de litígios (que podem apresentar queixas ao DOC e à FTC), perante o recém-criado Comité do Escudo de Proteção da Privacidade (iniciando uma arbitragem vinculativa) e, por fim, através da reação para os tribunais norte-americanos[44]. A grande novidade foi a criação de um Mediador para receber queixas interpostas por autoridades de controlo nacionais da UE em nome de cidadãos particulares quanto à prática de serviços de espionagem pelos EUA[45]. Este Mediador fará parte da estrutura administrativa do Governo dos EUA, respondendo perante o Secretário de Estado.

Por fim, para além de renovadas declarações relativas à supervisão da aplicação dos princípios por parte de autoridades como o DOC, a FTC e o *Department of Transportation*[46], foi acrescentada uma carta do *Director of National Intelligence*, que explica e presta garantias quanto ao modo de recolha de dados para efeitos de segurança nacional, ao abrigo de regras proporcionais quanto ao nível de interferência nos direitos dos particulares, e os direitos e meios de reação dos particulares nessas situações[47].

---

[43] *Idem*, pp. 52-67.

[44] *Idem*, pp. 9-12.

[45] Comissão Europeia, "Decisão de execução...", Anexo III, pp. 71-77.

[46] Comissão Europeia, "Decisão de execução...", Anexos IV e V, pp. 78-90.

[47] Comissão Europeia, "Decisão de execução...", Anexo VI, pp. 91-108.

4. Os princípios de *Privacy Shield* face ao direito da União Europeia

4.1. A compatibilidade do Privacy Shield *face aos critérios do acórdão* Schrems

Na secção II analisámos o quadro normativo de normas fundamentais e secundárias que se aplicam à proteção de dados. Vimos que, fora certas exceções, a regra geral é a de que só podem ser autorizadas transferências de dados para países terceiros desde que tais países disponham de um nível de proteção adequado. Deve entender-se por adequado, segundo o TJ, que o país terceiro em causa garanta um *quadro de proteção substancialmente equivalente* ao da UE. Esta avaliação sobre a adequação deve ser efetuada tendo em conta não só as normas abstratas aplicáveis mas, principalmente, a sua efetivação prática. O TJ considerou ainda que para um sistema jurídico garantir um nível de proteção substancialmente equivalente ao da UE deve preencher três critérios. Em primeiro lugar, o sistema deve ser eficaz, ou seja, estabelecer um nível de coerção suficiente que obrigue os seus aderentes à sua observação estrita. Em segundo lugar, o sistema deve ter como objetivo principal a proteção dos direitos de privacidade dos titulares de dados, sendo qualquer derrogação a este princípio excecional e exercida segundo requisitos de necessidade e de proporcionalidade. Em terceiro lugar, o sistema deve estabelecer meios judiciais de reação ao dispor dos titulares contra possíveis violações dos seus direitos.

Vimos igualmente que o TJ considerou no acórdão *Schrems* que estes critérios não estavam a ser preenchidos pois existiam demasiadas derrogações possíveis face a uma primazia do princípio de segurança nacional. Além do mais, o TJ entendeu que não existiam garantias jurídicas suficientes que impedissem uma recolha e um tratamento generalizado de dados. Desta forma, tal tratamento não obedecia a critérios de estrita proporcionalidade e necessidade. O TJ também considerou que os particulares não tinham direito, na prática, a uma tutela jurídica efetiva face a estas interferências de autoridades públicas. Assim, parece que a questão que mais preocupa o TJ não é tanto o tratamento *per se* de dados por empresas privadas, mas sim o seu tratamento pelas autoridades públicas norte-americanas, em especial as agências de informação e de segurança nacional. Também vimos que previamente ao acórdão *Schrems* existiu uma comunicação da Comissão Europeia que identificou deficiências no *Safe Harbor* e apresentou

recomendações. No entanto, a possibilidade de acesso a dados por parte de entidades públicas americanas não era alvo de tanto destaque como no julgamento do TJ. As principais preocupações da Comissão tinham que ver mais com a adesão de empresas ao regime de *Safe Harbor* e com a efetiva supervisão das autoridades norte-americanos quanto ao cumprimento desses princípios e aos meios de reação ao dispor dos particulares.

Na nossa análise geral ao sistema de *Privacy Shield* vimos que foram introduzidos novos princípios e obrigações para as empresas, em especial quanto às questões de transparência e de recurso[48]. Neste sentido, parece que as preocupações da Comissão, face ao nível de proteção *micro* (perante as empresas) foram salvaguardas. Cabe-nos no entanto verificar se as preocupações do TJ, quanto ao nível de proteção *macro* (perante o Estado), e essas sim decisivas quanto à interpretação a dar às normas da Diretiva sobre os limites do juízo de adequação, foram ou não objeto de resposta no *Privacy Shield*.

Comecemos por verificar o primeiro critério, relativo à eficácia. O *Privacy Shield* estabelece em várias disposições o compromisso das autoridades regulatórias norte-americanas, mormente o DOC, de supervisionar de forma estrita o cumprimento dos princípios e obrigações das empresas[49]. No entanto, nenhum destes compromissos refere qualquer poder efetivo destas entidades regulatórias face a possíveis interferências de outras entidades públicas, em particular de índole militar ou informativa. É verdade que se verifica um esforço na Decisão *Privacy Shield* de fundamentar de forma desenvolvida e aprofundada as capacidades do ordenamento jurídico norte-americano de regular eficazmente a aplicação dos novos princípios. É preciso relembrar, no entanto, que o sistema norte-americano continua assente na autocertificação, pelo que cabe ainda às empresas aderir e adotar políticas

---

[48] Para uma análise mais extensa do Privacy Shield, v. Monteleone, Shara e Puccio, Laura. "From Safe Harbour to Privacy Shield: Advances and Shortcomings of the New EU-US Data Transfer Rules, *European Parliament Research Service*, 2017, pp. 1-36.

V. igualmente a contribuição de Andrade de Jesus, Inês Oliveira. "O direito à proteção de dados pessoais e o regime jurídico das transferências internacionais de dados: a proteção viaja com as informações que nos dizem respeito?" e, em particular, pela análise crítica do valor normativo do *Privacy Shield*, de Rodrigues de Oliveira, Ricardo. "What's in a name? Uma breve análise do nível de protecção adequado no âmbito das transferências de dados pessoais dos cidadãos da UE para países terceiros", publicado neste Anuário.

[49] Comissão Europeia, "Decisão de execução...", pp. 40-44.

de proteção de dados, sem interferências das autoridades reguladoras. Ou seja, só será possível verificar o critério da eficácia em concreto após a entrada em vigor do sistema. Assim, apesar de existirem declarações de que existirá uma supervisão e aplicação mais eficaz do *Privacy Shield* do que houve do *Safe Harbor*, essas não passam de meras expressões de intenções de conduta. Neste sentido, coloca-se a dúvida sobre se a preocupação expressa pelo TJ no acórdão *Schrems* quanto à existência de um sistema de proteção eficaz estará completamente resolvida. Tal preocupação, parece-nos, só poderá ser resolvida através de uma análise concreta dessa supervisão, na prática.

Passemos para o segundo critério. O *Privacy Shield* continua a manter *ipsis verbis* as derrogações aos seus princípios para fins de segurança nacional. Assim, a adesão aos mesmos:

> [P]ode ser limitada: a) na medida necessária para observar requisitos de segurança nacional, interesse público ou execução legal, b) por legislação, regulamento governamental ou jurisprudência que criam obrigações contraditórias ou autorizações explícitas, desde que, no exercício de tal autorização, uma organização possa demonstrar que o seu incumprimento dos princípios se limita ao necessário para respeitar os legítimos interesses superiores avançados por essa autorização, ou c) por exceção ou derrogação prevista na diretiva ou nas normas de direito interno dos Estados-Membros, desde que a aplicação das referidas exceções ou derrogações ocorra em contextos comparáveis[50].

A questão continua a colocar-se quanto ao carácter excecional destas derrogações e da necessidade e proporcionalidade na sua aplicação. Há um esforço grande no *Privacy Shield*, particularmente expresso no anexo VI na carta do *Director of National Intelligence*, para descrever e informar sobre todos os direitos e regras dos titulares de dados tratados pelas agências de investigação, bem como sobre os meios de fiscalização política de tal atividade e da proporcionalidade dos mecanismos utilizados. A Comissão vem acrescentar que considera que desde 2013 este quadro jurídico de "proteção eficaz de dados contra a ingerência ilegal e o risco de abuso" foi bastante reforçado[51]. Este reforço verifica-se, na opinião da Comissão, com a aprovação da PPD-28 de 2014, que estabelece vários deveres que os

[50] *Idem*, p. 49.

[51] *Idem*, p. 13.

serviços de informação americanos devem cumprir quando tratam dados[52]. Chama-se igualmente a atenção para o facto de ter sido aprovado o *USA Freedom Act* em 2015, que veio alterar legislação sobre segurança nacional e combate ao terrorismo (*Patriot Act* e o FISA) no que respeita à eliminação da recolha massificada de dados.

Apesar destes esforços, mantém-se ainda a dúvida sobre se estes compromissos são suficientes ou não para satisfazer os critérios normativos estabelecidos pelo TJ. Existem três elementos que continuam a suscitar preocupações. O primeiro tem que ver com a recolha de informação de forma generalizada. Diz a Comissão que ao abrigo da legislação norte-americana "as informações de origem eletromagnética podem ser recolhidas exclusivamente nos casos em que exista um objetivo de espionagem externa ou de contra-espionagem ou para apoiar missões nacionais e departamentais[53]", e não para qualquer outro fim. Nesse âmbito, os serviços de informação "devem [ao abrigo da PPD-28], por vezes recolher informação de origem eletromagnética em larga escala em determinadas circunstâncias, por exemplo, para identificar e avaliar ameaças novas ou emergentes", embora tenham de dar prioridade a métodos alternativos de recolha seletiva[54]. A recolha alargada só pode ser efetuada por falta de meios técnicos ou operacionais que impeçam a recolha individualizada. Ora tal descrição da PPD-28 não parece estabelecer, de forma clara, certa e precisa, que a recolha generalizada de dados só será utilizada em casos altamente excecionais. Os serviços de informação devem dar prioridade a meios menos lesivos, mas isso não exclui a possibilidade de, em certos casos (cuja excecionalidade assenta somente em meios técnicos) poderem recorrer à recolha dados de forma massificada e generalizada. A legislação americana (quer o FISA, o programa *PRISM* e o *American Freedom Act*) também não é clara quanto aos limites e alcance dos poderes das autoridades americanas neste ponto.

O segundo elemento tem que ver com a questão do período de retenção de dados. Segundo as declarações que compõem o Privacy Shield, é possível que os serviços de informação possam reter os dados por um período máximo de cinco anos, sem qualquer aparente motivo[55]. Ora, isto vai contra aquilo

---

[52] *Idem*, p. 14.

[53] *Ibidem*.

[54] *Idem*, p. 15.

[55] *Idem*, p. 19.

que é considerado como sendo proporcional pelo TJ. Segundo a opinião do douto tribunal no acórdão *Digital Rights*, a retenção de dados por um período largo tem de obedecer a um "critério objetivo por modo a assegurar que está limitado ao que é estritamente necessário[56]". No entanto, não há qualquer menção na Decisão *Privacy Shield* a critérios que justifiquem a retenção por tal período de tempo. Assim, falta claridade e precisão numa matéria de especial importância. A Comissão considera que "esta prática [dos EUA] está conforme à norma fixada pelo Tribunal de Justiça no acórdão *Schrems*, segundo o qual uma legislação que envolva uma ingerência nos direitos fundamentais garantidos pelos art. 7.º e 8.º da Carta deve impor 'um mínimo de exigências". Mas temos dúvidas que assim seja, visto que ainda existe um elevado grau de dúvida e de imprecisão relativamente às possibilidades de interferência dos serviços secretos norte-americanos nos direitos dos particulares, em particular quanto à recolha generalizada de dados, o seu tratamento e acesso e à sua preservação. Aliás, apesar da abertura e disponibilidade para maiores explicações, a importância detalhada de questões relacionadas com atividades de serviços de informação no *Privacy Shield* parece indicar o quão importante é este princípio para os norte-americanos. Tal é que a AEPD vem, no seu parecer, questionar se a centralização deste princípio de segurança nacional na Decisão *Privacy Shield* não vem antes "legitimar a rotina" de recolha e de investigação, mesmo que estabeleça alguns limites à atividades de investigação e recolha de dados[57]. Ou seja, coloca-se a questão de saber se a exceção de segurança nacional não se torna, no *Privacy Shield*, na regra, e a proteção de direitos de privacidade na exceção, a contrário daquilo que é prescrito no acórdão *Schrems*.

O terceiro e último elemento tem que ver com o problema da tutela judicial efetiva. Os princípios de *Privacy Shield* estabelecem uma série de mecanismos de recurso ao dispor dos particulares. No entanto, todos estes mecanismos, exceto o último de acesso aos tribunais nacionais norte-americanos, dizem respeito à reação contra o tratamento de dados por empresas aderentes ao *Privacy Shield* e preconizam como meio principal a arbitragem. Como refere a AEPD, não há a possibilidade de intentar uma ação em solo europeu, o que garantiria uma tutela judicial dos particulares

---

[56] Casos C-293/12 e C-594/12, *Digital Rights Ireland*, paras. 63 e 64.

[57] Autoridade Europeia para a Proteção de Dados, "Opinion 4/2016...", cit., p. 7.

mais efetiva[58]. Mas mais problemático é o facto, mais uma vez, do sistema norte-americano não conter nenhum mecanismo claro e preciso ao dispor dos particulares para reagir contra o possível acesso aos dados por parte de autoridades públicas norte-americanas. Como diz a AEPD, "parecem existir vários instrumentos de recurso no direito norte-americano mas nenhum cobre de forma adequada todas as instâncias em que o governo pode aceder a dados pessoais[59]". Parece-nos que neste caso cabe aos particulares utilizar uma de duas vias: ou os tribunais norte-americanos, ou recorrer ao Mediador de proteção de dados, estabelecido ao abrigo do Anexo (III) da Decisão *Privacy Shield*. Mas esta situação também é problemática. Por um lado, a utilização de tribunais nacionais norte-americanos implica um custo para os cidadãos europeus que pode ser incomportável, dado o facto de se terem de deslocar e contratar serviços jurídicos para conseguir reagir num sistema forense bastante diferente do europeu. Por outro lado, o mediador é uma entidade que se encontra dentro da estrutura administrativa da Secretaria de Estado norte-americana. Ou seja, é nomeado pelo Secretário de Estado, que é um órgão executivo e que tem competência para tratar da política externa dos EUA. Não parece que estejam assim preenchidos os mínimos requisitos de independência e imparcialidade do Mediador face ao poder executivo norte-americano, ao qual pertencem as agências de informação. É um mecanismo meramente administrativo, que precisaria de mais desenvolvimentos para garantir a eficaz tutela judicial dos particulares de forma equivalente ao prescrito no art. 47.º da CDFUE[60].

4.2. O problema da avaliação efetiva do Privacy Shield

A análise anterior sobre o sistema de *Privacy Shield* centrou-se em normas jurídicas e sua consideração em abstrato. No entanto, como vimos no acórdão *Schrems*, a decisão de adequação tem de ter em conta um critério de eficácia, que considera em especial a execução e aplicação prática do sistema de proteção de dados pessoais do país terceiro. Este juízo é mais

---

[58] *Idem*.

[59] *Ibidem* (tradução do autor).

[60] *Idem*, "Opinion 4/2016...", p. 8; G29, "Opinion 01/2016", cit., p. 57.

complicado de fazer de momento, do ponto de vista científico, pois não existem ainda dados suficientes sobre a aplicação do *Privacy Shield* durante o seu curto período de vigência. Um juízo sobre a eficácia do sistema feito neste momento será necessariamente uma prognose, baseada simplesmente nos diplomas normativos e numa análise contextual e histórica sobre qual poderá ser a verdadeira capacidade de execução destas normas. No entanto, estamos em crer que quer os dados disponíveis por via da decisão de adequação e do contexto jurídico-político atual (e neste sentido, devido a algumas ações concretas do Governo norte-americano) proporcionam algumas informações para conseguir projetar pelo menos alguns desafios à execução do sistema, com uma margem suficientemente legítima de dúvida que pode ter efeitos importantes na capacidade de sucesso do *Privacy Shield*.

A decisão de adequação da Comissão considera que os EUA oferecem um sistema de proteção substancialmente equivalente com base numa análise do seu sistema jurídico de proteção de dados. Esta análise é fundamentada não só por referência a legislação americana e outros atos normativos de cariz executivo-administrativo, como a PPD-28, mas igualmente devido às comunicações em anexo dos diretores das entidades públicas norte-americanas. Ora estas cartas pretendem vincular as entidades em causa à execução dos princípios de *Privacy Shield*. No entanto, tal declaração não é um instrumento com força de lei[61]. Ou seja, o poder vinculativo destas declarações é reduzido, pois são meras declarações de intenções. Basta que os titulares das direções ou os órgãos políticos superiores da administração norte-americana mudem de posto para que uma nova direção possa dar ordens diferentes da anterior. Visto que o sucesso dos princípios do *Privacy Shield* está dependente da sua efetivação prática por parte dos reguladores, dentro do sistema de auto-certificação, e das autoridades de segurança nacional, coloca-se o problema de saber até que ponto é que estas declarações vão ou não ser cumpridas.

Estas declarações pertencem a órgãos executivos que seguiam uma determinada estratégia política definida por uma administração norte-americana liderada por um membro do Partido Democrata, Barack Obama. O programa e agenda política deste Presidente evidenciava uma postura

[61] *Idem*, p. 7.

pró-globalização, aberta à cooperação internacional e económica. Cerca de três meses após a aprovação da Decisão *Privacy Shield* houve eleições nos EUA, sendo o vencedor das eleições um candidato do Partido Republicano, Donald Trump. Enquanto candidato o Presidente Trump defendeu posições políticas completamente contrárias às do seu antecessor Barack Obama, advogando um maior protecionismo económico, uma visão mais nacionalista e anti-globalização. Neste sentido, tem procurado tomar medidas para combater a entrada de cidadãos estrangeiros nos EUA, medidas essas que levantam muitas dúvidas quanto a possíveis discriminações religiosas ou étnicas[62]. Apesar de tais tentativas terem sido bloqueadas pelos tribunais[63], não é seguro que a atividade das agências de informação para recolher dados de imigrantes e cidadãos estrangeiros não aumente com esta nova postura protecionista da administração Trump. Ao mesmo tempo têm sido preparadas medidas pelo Congresso norte-americano para eliminar regulação de práticas comerciais privadas, com importantes incidências nos direitos de proteção de dados dos cidadãos[64]. Coloca-se desta forma a dúvida de saber se as declarações de *Privacy Shield* serão ou não cumpridas na prática pelas autoridades norte-americanas.

Conclusão

Os requisitos estabelecidos pelo TJ no acórdão *Schrems* sobre qual o entendimento jurídico a dar ao conceito de "nível de proteção adequado" acabam por delimitar a adoção de decisões de adequação sobre países que não garantam, na prática, a proteção dos direitos dos particulares da

---

[62] Presidente dos Estados Unidos da América, "Executive Order Protecting The Nation From Foreign Terrorist Entry Into The United States. Disponível em: <https://www.whitehouse.gov/the-press-office/2017/03/06/executive-order-protecting-nation-foreign-terrorist-entry-united-states> (acedido a 25/10/2017).

[63] *BBC*, "Trump travel ban: Hawaii judge places indefinite hold", de 30 de março de 2017. Disponível em: <http://www.bbc.com/news/world-us-canada-39439595> (acedido a 25/10/2017).

[64] *The Independent*, "US Senate votes to allow sale of people's browsing history without consent", de 23 de março de 2017. Disponível em: <https://www.independent.co.uk/life-style/gadgets-and-tech/news/us-senate-internet-privacy-bill-vote-sell-consumer-data-browsing-history-a7646981.html> (acedido a 25/10/ 2017).

mesma forma que na UE[65]. A Decisão de *Privacy Shield* procura demonstrar que o novo sistema de princípios acordado com os EUA preenche todos os critérios e que se trata de uma proteção substancialmente equivalente à que os particulares gozam na UE. Existe, de facto, uma nova precisão e desenvolvimento quer ao nível dos princípios que as empresas devem seguir, quer ao nível dos controlos que as entidades de supervisão vão exercer. No entanto, existem elementos importantes da Decisão de *Privacy Shield* que continuam a ser problemáticos e a conflituar com o entendimento do TJ em *Schrems* e, assim, com o direito da UE. Ainda se estabelece um primado do princípio de segurança nacional face ao primado do respeito pela intimidade privada, ainda existe a possibilidade de recolha generalizada de dados, e não existem ainda mecanismos de reação suficientemente adequados ao dispor dos particulares perante interferências estatais. Parece-nos, deste modo, que a Decisão de *Privacy Shield*, mais do que cumprir com os requisitos delineados no acórdão *Schrems* procura resolver as questões levantadas pela Comissão na sua Comunicação.

Cabe aqui dizer que o problema do juízo de compatibilidade do *Privacy Shield* com o direito da União (já) não é apenas uma questão a ter em conta em abstrato. Isto porque em setembro e outubro de 2016 foram intentadas duas ações de anulação junto do TG para avaliar da validade do sistema face ao direito da União Europeia[66]. A primeira ação foi apresentada pela organização não-governamental Digital Rights Ireland[67], e a segunda pela

---

[65] Há quem questione não só a interpretação do TJ mas também as consequências da mesma. v. a discussão entre Richard Epstein e Martin Scheinin na European Constitutional Law Review. Epstein, Richard A. "The ECJ's Fatal Imbalance Its Cavalier Treatment of National Security Issues Poses Serious Risk to Public Safety and Sound Commercial Practices" e Scheinin, Martin. "Towards Evidence-Based Discussion on Surveillance: A Rejoinder to Richard A. Epstein", *European Constitutional Law Review,* vol. 12, n.º 2, 2016, pp. 330-348.

[66] *Politico*, "Privacy shield data agreement challenged before EU court", de 27 de outubro de 2016. Disponível em: <http://www.politico.eu/article/privacy-shield-data-agreement--challenged-before-ecj/> (acedido a 24/04/2017); EurActiv, "EU-US Privacy Shield pact faces second legal challenge", de 3 de novembro de 2016. Disponível em: <http://www.euractiv.com/section/digital/news/eu-us-privacy-shield-pact-faces-second-legal-challenge/> (acedido a 25/10/2017).

[67] Recurso interposto em 16 de setembro de 2016 – Digital Rights Ireland/Comissão, Processo T-670/16. A acção foi julgada inadmissível pelo TJ a 22 de novembro de 2017. V. Disponível em: <http://curia.europa.eu/juris/document/document.jsf?text=&docid=19714

organização não-governamental La Quadrature du Net[68]. Acrescente-se a isto os desenvolvimentos que a aplicação de políticas aguerridas de segurança nacional e de desregularização de proteções de utilizadores de dados por parte da Administração Trump e é difícil de prever o futuro do *Privacy Shield* para lá de uma grande nuvem de incerteza, apesar de ser o sistema que está atualmente em prática[69].

O problema de uma regulação transfronteiriça de proteção de dados é tentar satisfazer quatro preocupações. Por um lado, é preciso salvaguardar as liberdades económicas e de desenvolvimento empresarial, mas garantindo um nível de proteção adequado para os direitos de intimidade privada dos particulares, bem como uma proteção da segurança nacional e, com tudo isto, manter boas relações diplomáticas e comerciais com países terceiros, em especial com grandes potências internacionais que partilham na sua base constitucional e democrática o compromisso liberal e cosmopolita de proteção dos direitos fundamentais[70]. Resolver esta quadratura do círculo é o grande desafio desta área, ao qual o *Privacy Shield*, perante o entendimento do TJ sobre a primazia dos direitos individuais face aos outros interesses, parece não conseguir dar resposta.

1&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=812481> (acedido a 20/12/2017).

[68] Recurso interposto em 25 de outubro de 2016 – La Quadrature du Net e o./Comissão, Processo T-738/16.

[69] Apesar da incerteza, o Privacy Shield passou na primeira revisão anual efetuada pela Comissão. v. Directorate General of Justice and Consumers, "First Annual Review of the EU-U.S. Privacy Shield". Disponível em: <http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=605619> (acedido a 25/10/2017). No entanto, apesar do relatório ser favorável e à melhor supervisão por parte das autoridades regulatórias, foram identificadas situações que precisam de maior definição, relativamente a procedimentos internos de investigação e vigilância. O facto de não ter sido ainda nomeado um Mediador foi igualmente considerado problemático. A Comissão disse que continuaria a analisar de perto a situação. v. Comissão Europeia"Report From the Commission to the European Parliament and the Council on the first annual review of the functioning of the EU–U.S. Privacy Shield". Disponível em: <http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=605619> (acedido a 25/10/2017).

[70] Sobre este ponto, v. Lucas Pires, Martinho, "The shortcomings of the EU framework for transnational data transfers and the need for an internationalist approach", LUISS School of Governance Working Paper Series 43/2017. Disponível em: <http://sog.luiss.it/sites/sog.luiss.it/files/SOG%20Working%20Papers%20WP43%20-%202017%20Pires_0.pdf>. (acedido a 20/12/2017).