CYBERLAW

by CIJIC

Cyberlaw by CIJIC, ***Direito: a pensar tecnologicamente.***

# CYBERLAW by CIJIC

**EDIÇÃO N.º XI – MARÇO DE 2021**

**REVISTA CIENTÍFICA SOBRE CYBERLAW DO CENTRO DE INVESTIGAÇÃO JURÍDICA DO CIBERESPAÇO – CIJIC – DA FACULDADE DE DIREITO DA UNIVERSIDADE DE LISBOA**

CYBERLAW
by CIJIC



**CIJIC:** CENTRO DE INVESTIGAÇÃO JURÍDICA DO CIBERESPAÇO

**ISSN 2183-729**

CYBERLAW by CIJIC

## NOTAS DO EDITOR:

Finda Março do ano de 2021.

Passou um ano desde que o mundo se confinou, massivamente. Fechados, em casa, nunca como a partir disto o acesso à *Internet* se nos desvelou como um direito humano fundamental.

O sonho de uma *internet* livre, neutral, aberta, inclusiva, universal será possível?

Provavelmente muitos de nós, que navegam por ela, num ou noutro canto de conversação e/ou *stop by* possível a partir de um dos nossos hodiernos cárceres físicos, já nos deparámos com um curioso grafo. Nele consta uma espécie de sondagem onde à pergunta: *"Quem fez mais pela digitalização da sua organização no último ano?"*, a percentagem do vencedor surpreende.

Não, não foi o CEO da organização. Também não, não foi o CISO (quando as organizações os têm). Sim, também não foi nenhum diretor de nenhum departamento da organização.

O principal responsável, sim, foi ela: a pandemia de covid-19.

É inegável. A pandemia acelerou o processo de digitalização de grande parte das interações humanas, sejam elas de qualquer natureza, escola, comércio, socialização.

Não obstante, por mais benefícios que este *input*, à *força bruta*, tenha trazido, a humanidade tem ainda um caminho muito longo para percorrer.

Num plano macro, que convoca a humanidade, combater ferozmente a exclusão digital, com particular enfoque nos reversos, *i.e.*, mais novos e mais velhos; sociedades desenvolvidas/mais pobres.

E se o acesso não é universal (sê-lo-á algum dia?), plural, em condições idênticas, inclusivo…também não deixará de ser preocupante, dentro daqueles que podem aceder, o número de indivíduos com falta de formação, com falta de um mínimo de educação/formação para usufruir da Rede.

Atente-se, porém, num plano micro, por exemplo, no caso português.

Entregue, neste último dia de Março de 2021, o RASI2020[1], nele despontam algumas evidências sobre a temática da falta de educação para o *ciber*. Os crimes praticados na e pela *Internet*, nomeadamente, *phishing*, *vishing*, *ransomware* e extorsão[2], em passo crescente, decorrem de variadas falhas ao nível do utilizador. Sobressai, da leitura crua dos números, uma inexistente cultura de ciberhigiene. A facilidade de promoção de engenharias sociais avulsas. É esta omissão de cibereducação responsável pela inabilidade em detetar o logro e burlões, em actividade fervorosa. No compasso da oferta/procura de produtos através do digital, se as trocas aumentam exponencialmente, paralela e em acompanhamento, as situações de fraude, burla, roubo, *Money mules*, etc., *idem*.

As múltiplas deficiências ao nível do utilizador – o famoso factor humano é implacável - e a violência de uma *digitalização à força bruta* de uma grande maioria das organizações, combinadas… dão razão de ser à *tame joke* informática de que, *na prática, em termos de ataques e crimes informáticos, só há dois tipos de organizações: as que*

1 Disponível para consulta em: https://www.portugal.gov.pt/download-ficheiros/ficheiro.aspx?v=%3d%3dBQAAAB%2bLCAAAAAAABAAzNDQ1NAUABR26oAUAAAA%3d (último acesso 31MAR21)
2 *Vide* páginas 67 e ss do RASI2020.

*sabem que já foram atacadas e as que ainda não o sabem* (a premissa irónica é, infelizmente, igualmente válida para as pessoas singulares).

Torna-se inadiável que, paralelamente ao percurso do Direito no séquito da acelerada digitalização, as organizações, as pessoas, o Estado, entendam, decisiva e finalmente, a importância da segurança da informação[3].

Apaticamente, e em crise, as omissões perduram. Sedimentam.

Os alertas não chegam a bom porto. Provenham eles de serviços mais ou menos capacitados do Estado, sejam serviços secretos nacionais, sistema de segurança interna, observatórios…jaz, apenas, a constatação impotente de que "(…) *observa-se um aumento da espionagem através de ameaças persistentes, tecnologicamente avançadas, de origem estatal, direcionadas a importantes centros de informação do Estado. Uma das consequências da sofisticação enunciada, prende-se com a crescente dificuldade em destrinçar ataques informáticos para efeitos de crime económico ou de crimes de sabotagem, dirigidos a empresas e grupos de empresas com relevância no tecido empresarial nacional*."

No presente, de crescente digitalização, de cascata informacional, já todos sabemos que não é a quantidade de informação que serve à melhor tomada de decisão; é a qualidade. Mostra-se-nos angustiante o sublinhado de "*ameaças persistentes, tecnologicamente avançadas, de origem estatal, direcionadas a importantes centros de informação do Estado"*.

O Estado, como nunca, até como condição de promoção e prossecução geracional, tem o dever de defender um desígnio de soberania consubstanciado, precisamente, na superioridade informacional.

Conhecerá o Estado a capital importância da superioridade informacional?

Estará capacitado, humana e tecnologicamente, para proteger, o mais eficazmente possível, os seus mais valiosos *assets*, as suas infraestruturas mais críticas?

---

3 Ainda, no RASI2020 agora dado a conhecer, «(…) *No universo da ciberespionagem, registaram-se novos ciberataques contra infraestruturas críticas nacionais, com a finalidade de aceder a informação classificada, com valor político e económico."*», página 102.

Severa, a frieza dos parágrafos, no contexto pandémico Covid-19: "*No que concerne a outra das ameaças, i.e., as operações cibernéticas ofensivas, foram identificados agentes estatais e não estatais, visando entidades públicas e privadas, em particular no que respeitou à exploração de oportunidades…Verificaram-se inúmeros ciberataques registados contra instituições do setor da saúde, bem como operações de ciberespionagem contra entidades de investigação cientifica, particularmente envolvidas na pesquisa de terapêuticas e de vacinas contra a doença em apreço.*"

A segurança da informação, e a superioridade informacional que daí possa erigir, são, no contexto, de suma importância.

Infelizmente, as ameaças são múltiplas. Se, como veremos nesta nova edição, a Segurança da informação nas organizações(SiO) é tema fulcral, a erosão, de direitos fundamentais humanos, não descola de uma objetificação pronunciada da pessoa, do ser individual. Discreta, mas de forma expedita, as *oportunidades geradas pelo contexto pandémico*, têm servido para que o Estado arroje sistemas de videovigilância por múltiplas localidades nacionais[4]. A febre dos sistemas *CCTV* públicos segue a passo acelerado.

Em simultâneo, embora a aplicação *stayawaycovid* não tenha vingado, ainda, é certo que o controlo à distância da pessoa irá figurar, brevemente, em alguma medida legislativa. Notemos, ainda no contexto da pandemia, por exemplo, e em pleno estado de emergência, os níveis de mobilidade do cidadão. Com a proibição de circulação fora-do-concelho e a aproximação do tema festivo pascal, na semana de 25/26 de Março, acordámos com a notícia: "*Portugueses fogem para longe das restrições: um em cada dez dormiu a mais de 100 quilómetros de casa esta quinta-feira.*"[5].

4 Ainda no RASI2020, dentre renovações e novas autorizações, surgem destacadas 8 despachos de autorização de instalação de múltiplas cameras de videovigilância para localidades. Consultáveis a partir dos Anexos do relatório, Medidas legislativas, página 15 e ss.
Nota: entretanto, no início do mês de março 2021, foi-nos dada a conhecer a autorização para instalação de mais 216 cameras de videovigilância na cidade de Lisboa, para juntar às já existentes (o Bairro Alto já dispõe de sistema, por exemplo).

5 https://expresso.pt/sociedade/2021-03-26-Portugueses-fogem-para-longe-das-restricoes-um-em-cada-dez-dormiu-a-mais-de-100-quilometros-de-casa-esta-quinta-feira-b98a7df0 (último acesso 31MAR21).

A observação - próxima da realidade? - feita por uma consultora privada[6], revelando que mais de *um milhão de portugueses dormiu fora de casa*, curiosamente, não promoveu nenhum sobressalto jurídico. Nem social. A ordem continua serena. *Curiosamente*. Mas, não houve tratamento de dados pessoais para a revelação de tais estatísticas em mobilidade? Que finalidade jurídica prosseguiu a captura de tais dados? Que dados foram recolhidos? Foram coligidos de forma lícita? Que tratamento tiveram? Quais as garantias de anonimização e/ou minimização do tratamento?

Alguém questionou?

Alguém se indignou?

Não sendo a primeira vez que uma entidade privada analisa dados dos portugueses, em massa, sem qualquer tipo de reacção/oposição por parte destes, presumivelmente, como solução eficiente a tomar por parte do Estado, no futuro deveremos promover toda uma actividade concursal de fundos públicos para *investigação* - geral e abstrata - de *tendências*, *mobilidade*, *gostos e desejos* dos portugueses. Não que haja uma qualquer necessidade de uma finalidade concreta, lícita de sopeso. Afinal, o problema, de fundo, do sobressalto cívico e jurídico, da ordem, reside numa mera formalidade de *marketing*, o "publico não pode" vs. "privado tudo pode".

Acabemos prontamente com a folia[7].

O acesso a metadados são um problema para a acção das nossas secretas?

Do titular da acção penal, *tout court*, português?

---

6 Vejamos, por exemplo, o detalhe dos grafos sobre a evolução do confinamento e mobilidade em: https://www.pse.pt/evolucao-confinamento-mobilidade/ (último acesso 31MAR21).

7 Reparem na notícia: https://www.jornaldenegocios.pt/economia/impostos/amp/fisco-vai-ter-assistente-virtual-no-facebook-para-responder-as-duvidas-de-irs (último acesso 31MAR21).
Ora, a Autoridade Tributária portuguesa entende que a plataforma do Facebook é a melhor disponível *para tirar dúvidas a contribuintes nacionais.* Como todos sabemos, e somos *surpreendidos semanalmente*, o Facebook, provavelmente, já é conhecedor da informação fundamental e necessária dos seus utilizadores. Com este *passo de modernidade* da nossa AT, na prática, ao Facebook bastar-lhe-á agrupar a informação detida à contributiva, com os rendimentos declarados, das finanças portuguesas e... *Et voila*, vitracidade completa do cidadão. (quanto será o preço de cada miríade informacional de um contribuinte concreto que a AT poderá desembolsar? Haverá já um acordo bilateral entre a entidade privada e a AT?)
É, pois, tempo de assumirmos já a cedência gratuita dos nossos dados pessoais às entidades privadas e, a partir daí, o Estado seja profícuo no controlo de todas as nossas actividades sem qualquer tipo de sobressalto jurídico ou social.

Renunciemos à recolha de torrentes de dados pessoais às entidades privadas, assumamos a bonomia do *surveillance capitalism*, encapotando o próprio "*estado de vigilância*", e vivamos felizes.

E ordeiros. Sem sobressaltos.

A justificação, para esta aceitação social passiva e dócil, por parte de uma maioria de cidadãos, refletindo, denota muito do seu analfabetismo. Analfabetismo digital. Mas também social. A ordem das coisas apenas sobrepuja o ponto de partida. A liberdade individual é gratuitamente cedida a entidades privadas. Nunca ao Estado. A compressão de direitos fundamentais apenas terá de partir deste porto privado.

Aquiesçamos, afinal, mais de duzentos anos depois, a sociedade não compreende o ditame de que "*uma sociedade que troca um pouco de liberdade por um pouco de ordem acabará por perder ambas, e não merece qualquer delas*"[8].

Nesta nova edição da Cyberlaw by CIJIC, em consonância com os docentes do Mestrado em segurança da informação e direito do ciberespaço[9], tivemos o ensejo de provocar alguns discentes a reflexões sobre a realidade pungente que convoca a sociedade. No presente e para o futuro. Entre a segurança da informação nas organizações (SiO), a consciencialização dos funcionários das organizações para a temática, o factor humano na SiO; dados pessoais em *Schrems II* e acesso a metadados por parte do MP sem um suspeito determinado ou determinável, *not/net neutrality*, os discentes procuraram reunir algumas interjeições que, como já demos conta oportunamente, ajudem a mitigar a desigual compreensão, a despertar a consciencialização individual para promoção de um combate ao analfabetismo digital.

Trazemos, também, a participação de proeminentes juristas brasileiros que acederam ao nosso convite para dissertarem sobre a lei geral de proteção de dados brasileira assim como sobre o fenómeno do *stalking* em contexto laboral inclusive em ambiente digital.

8 Thomas Jefferson (1743-1826), carta a James Madison.
9 https://fenix.tecnico.ulisboa.pt/cursos/msidc

Resta-me, assim e por fim, agradecer a todos quantos contribuíram para mais esta nova edição da Revista, pelo esforço, pela disponibilidade, pela obra, endereçando a todos, em nome do Centro de Investigação Jurídica do Ciberespaço – CIJIC – da Faculdade de Direito da Universidade de Lisboa, um merecidíssimo: - Muito Obrigado.

Cyberlaw by CIJIC, ***Direito: a pensar tecnologicamente*.**

**Boas leituras.**

Lisboa, FDUL, 31 de Março de 2021

Nuno Teixeira Castro


# PRIVACY SHIELD vs. ACÓRDÃO C-311/18 - *"SCHREMS II"*

**CATARINA CONDE NOGUEIRA** *

* Mestranda em segurança da informação e direito ciberespaço.

## RESUMO

A uniformização da proteção dos direitos fundamentais dos cidadãos europeus, na transferência dos seus dados pessoais entre a União Europeia e os Estados Unidos da América, representa um desafio na era digital. Na tentativa de garantir um nível de proteção adequado na transferência transatlântica destes dados, a 12 de julho de 2016, a Comissão Europeia estabeleceu a Decisão de Adequação (UE) 2016/1250, mais conhecida como Privacy Shield UE-EUA. Apesar de terem subsistido dúvidas quanto à sua compatibilidade com os requisitos do RGPD, o Privacy Shield esteve em vigor até 16 de julho de 2020, data em que o Tribunal de Justiça da União Europeia declarou inválida a Decisão de Adequação 2016/1250, na decisão que ficou conhecida como Schrems II, a qual veio originar um novo panorama na transferência de dados pessoais para países terceiros.



**Palavras-Chave**: RGPD; Transferência de dados pessoais para países terceiros; Proteção de dados pessoais; *Privacy-Shield* UE-EUA; *Schrems* II.

## ABSTRACT

Ensuring a standardized protection of the European citizens' fundamental rights, when transferring their personal data between the European Union and the United States, represents a challenge in the digital age. To ensure an adequate level of protection in the transatlantic transfer of these data, on 12th July 2016, the European Commission established the Adequacy Decision (EU) 2016/1250, more widely known as the EU-US Privacy Shield. Although there were some doubts regarding its compatibility with the GDPR's requirements, the Privacy Shield was in force until 16th July 2020, when the Court of Justice of the European Union declared the Adequacy Decision 2016/1250 invalid, in the decision known as Schrems II, leading to a new approach for personal data transfer to third countries.

**Keywords**: Personal data transfer to third countries; Data protection; Privacy-Shield UE-EUA; Schrems II.

## 1. Introdução

Nos últimos dois anos, mais precisamente desde a implementação do Regulamento Geral de Proteção de Dados (RGPD), a 25 de maio de 2018, tem existido um maior interesse e uma preocupação crescente, tanto por parte dos cidadãos como das empresas, no que diz respeito à privacidade e à proteção dos dados pessoais, bem como a aspiração notória da União Europeia (UE) em afirmar-se como uma referência na proteção jurídica dos titulares de dados.

O Regulamento (UE) n.º 2016/679, relativo à proteção das pessoas singulares no que diz respeito ao tratamento dos seus dados pessoais e à livre circulação desses dados, de 27 de abril de 2016, veio reforçar os direitos fundamentais dos cidadãos da UE na era digital e, de certa forma, minimizar a fragmentação que existia. Este Regulamento Geral de Proteção de Dados aplica-se ao tratamento de dados pessoais efetuado no âmbito das atividades de empresas ou entidades com sucursais estabelecidas na UE, independentemente do local onde os dados são efetivamente processados, bem como ao tratamento de dados pessoais de titulares residentes na UE, efetuado por empresas constituídas fora da UE que ofereçam bens ou serviços a esses titulares ou qualquer tratamento relacionado com o controlo do comportamento destes[1].

No novo mundo virtual, a informação tende a circular sem constrangimentos espaciais, fruto do avanço tecnológico, do qual beneficiam não só os cidadãos, mas também as empresas. Atualmente, a transação de dados pessoais integra as atividades diárias das empresas em todos os setores da economia, tratando-se de uma tendência em crescimento, pelo que a entrada em vigor do RGPD trouxe novas preocupações a todas as empresas que, no âmbito do seu negócio, transferem dados pessoais[2].

Note-se que, de acordo com o Capítulo V do RGPD, relativo às transferências de dados pessoais para países terceiros ou organizações internacionais, o Artigo 45.º

1 Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho: 32-33.
2 Jesus, I. 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? 72

"Transferências com base numa decisão de adequação" estabelece que a transferência de dados pessoais é possível, se a Comissão Europeia tiver decidido que o país terceiro ou a organização internacional em causa assegura um nível de proteção adequado. Nestes moldes, a transferência não exige autorização específica. O Artigo 46.º "Transferências sujeitas a garantias adequadas" acrescenta que, caso não tenha sido tomada qualquer decisão nos termos do Artigo 45.º, n.º 3, os responsáveis pelo tratamento ou os subcontratantes só podem transferir dados pessoais para um país terceiro ou uma organização internacional, se estes tiverem apresentado garantias adequadas e na condição dos titulares dos dados gozarem de direitos oponíveis e de medidas jurídicas corretivas eficazes.[3]

Resumindo, quando são transferidos dados pessoais para fora da UE, a proteção assegurada pelo RGPD deve manter-se. Assim, pautados pelo nível de exigência que a aplicação do RGPD trouxe, no que concerne à proteção de dados pessoais, e na ausência da decisão de adequação da Comissão Europeia, vários países passaram a adotar medidas idênticas de forma a alcançar a desejada *compliance* que permitisse a continuidade e o crescimento dos seus negócios. Por exemplo, o Brasil adotou a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709, de 14 de agosto de 2018, a qual apresenta semelhanças evidentes ao RGPD, tendo entrado recentemente em vigor, mais precisamente a 18 de setembro de 2020[4]. Outro exemplo a considerar, trata-se da primeira lei do Quénia relativa à proteção de dados pessoais, o *Data Protection Act*, com entrada em vigor a novembro de 2019, o qual, uma vez mais, vai ao encontro dos requisitos do RGPD, no que concerne à recolha, partilha e armazenamento de dados pessoais[5].

A uniformização do nível de proteção dos direitos fundamentais dos cidadãos europeus, na transferência dos seus dados pessoais entre a UE e os Estados Unidos da América (EUA), foco do presente trabalho, representa, sem dúvida, um desafio na era digital. Na tentativa de garantir um nível de proteção adequado, a 12 de julho de 2016, foi tomada a decisão de adequação do *Privacy Shield* UE-EUA. O *Privacy Shield* foi, então, o sistema que, desde 1 de agosto de 2016, procurou garantir *compliance* com os requisitos de proteção de dados pessoais, suportando, assim, o comércio transatlântico

3 Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho: 61-62.
4 Governo do Brasil - Ministério da Defesa. Lei Geral de Proteção de Dados – LGPD.
5 Okwara, E. Kenya takes important step toward in data protection.

destes dados[6], apesar de terem subsistido dúvidas quanto à sua compatibilidade com os requisitos do RGPD, conforme opinião publicada pela Autoridade Europeia para a Proteção de Dados a 30 de maio de 2016.[7] Recentemente, a 16 de julho de 2020, o Tribunal de Justiça da União Europeia (TJUE) declarou inválida a Decisão 2016/1250, relativa à adequação do nível de proteção assegurado pelo *Privacy Shield*, na decisão que ficou conhecida como *Schrems* II, a qual veio corroborar com o cenário de incompatibilidade[8]. Esta decisão é especialmente relevante para o futuro dos fluxos internacionais de dados, ao abrigo dos mecanismos de transferência estabelecidos no RGPD, tendo originado um novo panorama na transação de dados pessoais.

6 Privacy Shield Framework. Privacy Shield Program Overview.
7 Autoridade europeia para a Proteção de Dados. Opinion 4/2016 on the EU-U.S. Privacy Shield draft adequacy decision.
8 Tribunal de Justiça da União Europeia. Comunicado de Imprensa nº91/20 de 16 julho 2020 relativo ao Acórdão no processo C-311/18.

## 2. Privacy-Shield UE-EUA

### 2.1 Breve Enquadramento

Antes da implementação do *Privacy Shield* em 2016, vigoravam, desde o ano 2000, os princípios de privacidade do *Safe Harbor* estabelecidos na Decisão 2000/520[9], até serem considerados incompatíveis com o direito da UE pelo Tribunal de Justiça no acórdão *Schrems* I (cujos acontecimentos serão explicados no terceiro capítulo do presente trabalho)[10].

No que diz respeito ao enquadramento legal da Decisão *Safe Harbor*, esta teve como base a Diretiva da Comissão Europeia 95/46, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento dos dados pessoais e à livre circulação desses dados. À data já era reconhecida a necessidade de existir fluxos de dados pessoais além-fronteiras, no âmbito do desenvolvimento do comércio internacional. Essas transferências de dados para países terceiros seriam possíveis desde que estes garantissem um nível de proteção adequado, em função das circunstâncias associadas à transferência em causa, e que caso o país terceiro não oferecesse um nível de proteção adequado, a transferência dos dados pessoais deveria, então, ser proibida[11]. Neste sentido, deu-se a negociação entre a UE e os EUA relativamente aos princípios do *Safe Harbor*, a qual foi conduzida pela Comissão Europeia e pelo Departamento de Comércio dos EUA, com acompanhamento técnico do Grupo de Trabalho do Artigo 29.º[12](estabelecido precisamente no artigo 29.º da Diretiva da Comissão Europeia 95/46, o qual foi substituído pelo *European Data Protection Board* (EDPB) aquando da publicação do RGPD).

A Decisão *Safe Harbor* estabelecia os seguintes princípios: princípio de aviso, da escolha, da re-transferência, da segurança, da integridade dos dados, do acesso e da

9 Comissão europeia, Decisão 2000/520 relativa ao nível de proteção assegurado pelos princípios de 'porto seguro' e pelas questões e pelas respetivas FAQ emitidas pelo *Department of Commerce* dos Estados Unidos da América, de 26 de julho de 2000.
10 Pires, M. Algumas considerações sobre a compatibilidade do sistema de Privacy Shield com o direito da União Europeia à luz do acórdão *Schrems*: 93.
11 Comissão europeia, "Decisão da Comissão nos termos da Diretiva 95/46/CE, relativa ao nível de proteção assegurado pelos princípios de "porto seguro" e pelas respetivas questões mais frequentes (FAQ) emitidos pelo *Department of Commerce* dos Estados Unidos da América", de 26 de julho de 2000.
12 Comissão Nacional de Proteção de Dados, Parecer n.º 14/2000.

aplicação. Estes princípios eram de aplicação territorial nos EUA e a decisão do seu cumprimento era voluntária, assente na autocertificação das empresas, que teriam de agir em conformidade com os princípios definidos de forma a obterem e manterem os benefícios do *Safe Harbor* e poderem declará-los publicamente[13].

Sumariamente, a decisão de adequação do *Safe Harbor* foi anulada pelas seguintes razões: a sua aplicação, por parte das empresas dos EUA, não garantia um nível de proteção de dados pessoais semelhante ao existente e exigido pela UE; as autoridades norte-americanas não estavam vinculadas a esta Decisão; e, por fim, os dados pessoais de cidadãos europeus podiam, então, ser objeto de tratamento incompatível e desproporcional por partes destas autoridades[14].

Assim, tornou-se premente a revisão do sistema que estabelecia os princípios de privacidade na transferência de dados UE-EUA, na perspetiva do avanço tecnológico e consequente aumento exponencial do fluxo de dados verificado, de forma a garantir um nível de proteção adequado dos dados pessoais e respetivos titulares[15]. Com a elaboração do *Privacy Shield* procurou-se preencher as lacunas do sistema anteriormente em vigor, aumentando o nível de exigência quanto às obrigações das empresas com sede nos EUA, bem como quanto às garantias de supervisão e ainda clarificando o vínculo das autoridades norte-americanas a esta Decisão.

### 2.2 Caraterização, Âmbito e Princípios

O *Privacy Shield* UE-EUA trata-se de uma *framework* concebida pelo Departamento de Comércio dos EUA, em conjunto com a Comissão Europeia, com o intuito de fornecer às empresas, de ambos os lados do oceano Atlântico, um mecanismo fiável para cumprir os requisitos de proteção de dados pessoais, aquando da sua transferência da UE para empresas com sede nos EUA, garantindo, assim, que os cidadãos da UE continuem a beneficiar de medidas de proteção adequadas. Esta *framework* baseia-se num sistema de autocertificação, cujo processo será explicado com maior detalhe mais

13 Comissão Nacional de Proteção de Dados, Parecer n.º 17/2000.
14 Raposo, Sá Miranda & Associados, Safe Harbor: Perguntas e Respostas.
15 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: 3.

à frente neste trabalho, através do qual as empresas dos EUA assumem o compromisso de estabelecer e cumprir os princípios de privacidade definidos[16]. Assim, o *Privacy Shield* veio trazer novas obrigações que reforçaram a transparência no tratamento dos dados pessoais e facilitaram o exercício dos direitos dos titulares de dados, através da informação obrigatória aos mesmos relativamente às políticas das empresas, no que concerne à proteção de dados pessoais, bem como dos meios existentes para os titulares poderem reagir face ao tratamento dos seus dados pessoais[17].

A *Privacy Shield framework* encontra-se dividida em três capítulos, sendo o primeiro intitulado de "*Overview*", no qual, como o próprio nome indica, são definidos os contornos gerais do programa, assim como o âmbito da certificação segundo o mesmo. No Capítulo II, *"EU-U.S. Privacy Shield Principles*", são definidos os princípios para a proteção dos dados pessoais, os quais procuram garantir o nível de proteção adequado, aplicável a qualquer titular de dados da UE cujos dados sejam transferidos para os EUA, a saber [18]:

1. *Notice*
2. *Choice*
3. *Accountability for Onward Transfer*
4. *Security*
5. *Data Integrity and Purpose Limitation*
6. *Access*
7. *Recourse, Enforcement and Liability*

O primeiro princípio para a proteção dos dados pessoais, "*Notice*", traduz-se na obrigação por parte empresas certificadas de fornecerem informações chave relacionadas com o processamento de dados pessoais aos respetivos titulares, tais como a categoria dos dados recolhidos, a finalidade do tratamento, os direitos dos titulares de dados, entre outros. O segundo princípio, "*Choice*", confere aos titulares dos dados o direito de se oporem ao tratamento, por exemplo quando se verifica uma alteração na finalidade do

16 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: 3-4.
17 Pires, M. Algumas considerações sobre a compatibilidade do sistema de Privacy Shield com o direito da União Europeia à luz do acórdão Schrems: 106-107.
18 U.S. Department of Commerce. EU-U.S. Privacy Shield Framework Principles.

tratamento que seja compatível com a finalidade inicial. No entanto, este princípio não afeta a proibição dos tratamentos incompatíveis. O princípio seguinte, "*Accountability for Onward Transfer*", estabelece que qualquer transferência ulterior, ou seja, qualquer transferência de dados pessoais de uma empresa para um responsável pelo tratamento ou um subcontratante, independentemente de este se encontrar nos EUA ou num país terceiro (fora dos EUA e/ou da UE), só é possível para fins específicos e limitados. Na ocorrência destas transferências, deve ser garantido o mesmo nível de proteção acautelado pelos princípios do *Privacy Shield*. O princípio "*Security*" estabelece que as empresas que processam dados pessoais devem implementar medidas de segurança adequadas, as quais devem ter em consideração os riscos relacionados com o processamento em si e com a categoria de dados processados. No que concerne ao princípio "*Data Integrity and Purpose Limitation*", os dados pessoais devem ser exatos, completos, fiáveis e atuais, bem como limitados ao que é realmente relevante para o propósito do tratamento definido. De acordo com este princípio, os dados pessoais só podem ser conservados enquanto a sua utilização esteja conforme a finalidade do tratamento, no entanto, esta obrigação não impede as empresas aderentes ao *Privacy Shield* de continuarem a tratar os dados durante um período mais longo, caso esse tratamento sirva uma finalidade específica, tal como a análise estatística, o jornalismo ou o arquivamento no interesse público. Com o princípio "*Access"* fica então estabelecido que os titulares dos dados têm o direito de obter a confirmação, por parte das empresas, de que os seus dados pessoais estão a ser processados, bem como o direito a que estes lhes sejam comunicados sem demora injustificada. Para além disto, os titulares de dados devem poder alterar ou eliminar informações pessoais sempre que estas estejam incorretas ou tenham sido tratadas em violação dos princípios. Por último, o princípio *"Recourse, Enforcement and Liability"* determina que as empresas certificadas devem proporcionar mecanismos que assegurem a conformidade com os sete princípios do *Privacy Shield* e também formas de recurso para todos os titulares, cujos dados pessoais tenham sido tratados de modo não conforme[19].

No Capítulo III, *"EU-U.S. Privacy Shield Supplemental Principles*" foram ainda incluídos alguns princípios suplementares, os quais vêm complementar os princípios

19 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: 4-6.

anteriormente referidos, acrescentando ainda algumas obrigações às empresas certificadas, como por exemplo a obrigatoriedade de verificação da adequação das práticas de privacidade exigidas pelo *Privacy Shield*, quer através de autoavaliação quer de revisões com recurso a entidades externas[20].

Assim, os princípios de privacidade definidos no *Privacy Shield* foram considerados adequados pela Comissão Europeia, na medida em que, no seu conjunto, assegurariam um nível de proteção dos dados pessoais equivalente ao nível assegurado pelo RGPD e, portanto, as empresas dos EUA certificadas também iriam garantir um nível de proteção adequado dos dados pessoais transferidos da UE. Nestes moldes, o *Privacy Shield* viria, então, impedir o acesso indiscriminado aos dados dos cidadãos europeus e a vigilância generalizada dos utilizadores.

À luz deste acordo, o Departamento do Comércio dos EUA foi eleito como a entidade responsável pela monitorização das empresas certificadas, de forma a assegurar que as condições previstas no *Privacy Shield*, nomeadamente a aplicação eficaz dos princípios e as obrigações de transparência no tratamento, fossem cumpridas.

De referir ainda a criação, por parte do governo dos EUA, de um novo mecanismo de supervisão da ingerência da segurança nacional, nomeadamente o Mediador para o *Privacy Shield*, para tratar de eventuais queixas colocadas por autoridades de controlo nacionais da UE, em nome dos titulares dos dados no que diz respeito à prática de espionagem nos EUA[21].

### 2.3 Autocertificação de Empresas

A adesão ao *Privacy Shield*, por parte de empresas com sede nos EUA, é inteiramente voluntária e pressupõe a sua autocertificação anual através do site do Departamento de Comércio dos EUA. Neste processo anual, as empresas comprometem-se a aderir aos Princípios do *Privacy Shield*, a verificar a conformidade das suas políticas e práticas de privacidade e ainda a cooperar com as autoridades com poder de

20 Privacy Shield Framework. 7. Verification.
21 Pires, M. Algumas considerações sobre a compatibilidade do sistema de Privacy Shield com o direito da União Europeia à luz do acórdão Schrems: 107.

investigação e execução, nomeadamente a *Federal Trade Comission* (FTC), o *Department of Transportation* (DOT), ou qualquer outro organismo oficial americano, na verificação do cumprimento efetivo dos mesmos[22].

De acordo com o guia disponibilizado no site do *Privacy Shield*[23], para a autocertificação das empresas, deve ser tido em consideração, em primeiro lugar, que apenas as empresas com sede nos EUA e, portanto, sujeitas à jurisdição da FTC ou do DOT, são elegíveis para a participação neste programa. O segundo passo para a autocertificação prende-se com o desenvolvimento de uma política de privacidade em conformidade com os princípios do *Privacy Shield*, a qual deve ser estabelecida antes da submissão da candidatura para a autocertificação. Esta política deve refletir as práticas organizacionais para o processamento de informação, bem como os meios disponibilizados aos titulares de dados, no que diz respeito à utilização e divulgação dos seus dados pessoais. Ainda é exigido a existência de uma declaração do compromisso da empresa com os princípios do *Privacy Shield*, incluindo o *hyperlink* para o site do *Privacy Shield*, quando existir confirmação de que a submissão está completa. De acordo com o princípio "*Recourse, Enforcement and Liability*", as empresas devem também identificar o mecanismo de recurso independente a quem irão recorrer para investigar eventuais reclamações, o qual tem de estar forçosamente estabelecido antes da certificação. O mecanismo de recurso independente, cujo estabelecimento é verificado pelo Departamento de Comércio dos EUA antes da certificação, deve estar referido também na política de privacidade da empresa. Em adição aos passos anteriores, as empresas que participam no programa *Privacy Shield* UE-EUA, têm de pagar uma contribuição à *American Arbitration Association* (AAA), baseada na dimensão da organização, podendo situar-se entre os $250 e os $10.000 USD, a qual cobrirá os custos do *Arbitral Fund*[24], conforme previsto no Anexo I, "*Arbitration Mechanism*", do *Privacy Shield*. Este fundo permite financiar julgamentos de eventuais violações das obrigações das empresas certificadas para com os cidadãos europeus. Ainda relativamente aos procedimentos necessários para a autocertificação, as empresas devem garantir que têm um mecanismo de verificação *in place*, que inclua procedimentos de autoavaliação internos ou o recurso a entidades externas, que avaliem o seu nível de conformidade com os princípios do

22 Privacy Shield Framework. How to join Privacy shield (part 1).
23 Privacy Shield Framework. A Step-by-Step Guide to Self-Certification on the Privacy Shield Website.
24 American Arbitration Association. ICDR-AAA EU-U.S. and/or Swiss-U.S. Privacy Shield Arbitral Fund Contributions.

*Privacy Shield*. As empresas devem ainda nomear um responsável, dentro da sua organização, que trate de todas as questões relacionadas com a certificação, nomeadamente reclamações, pedidos de acesso, entre outros, com o compromisso de resposta dentro do prazo máximo de 45 dias. Por último, deve ser paga uma taxa de processamento da candidatura no valor de $375 USD. Portanto, este era o procedimento em vigor anterior à decisão que veio invalidar a adequação do *Privacy Shield*.

## 3. Acórdão C-311/18 - "*SCHREMS II*"

### 3.1 Contexto Anterior (*Schrems* I) e Principais Considerações

A decisão do Tribunal de Justiça da UE (Acórdão C-311/18), de 16 de julho de 2020, a qual ficou conhecida como *Schrems* II, veio invalidar a adequação do *Privacy Shield* quanto ao nível de proteção por este assegurado, relativamente aos dados pessoais de cidadãos europeus transferidos para os EUA.

Na verdade, este Acórdão do TJUE veio na sequência do Acórdão C-362/14, de 6 de outubro de 2015 (*Schrems* I) relativo à queixa apresentada por *Maximillian Schrems*, um cidadão austríaco, advogado e ativista, fundador da organização sem fins lucrativos NOYB (*none of your business*) - *European Center for Digital Rights*, o qual era utilizador do *Facebook* desde 2008. *M. Schrems* alegou que os seus dados pessoais, à semelhança daquilo que acontece com todos os utilizadores europeus, são, no todo ou em parte, transferidos pela *Facebook Ireland* para servidores pertencentes à *Facebook Inc.*, situados nos EUA, onde são objeto de tratamento [25]. As revelações de *Edward Snowden*, antigo colaborador da *National Security Agency* (NSA), uma agência de segurança pertencente à administração dos EUA, trouxeram a público as práticas de vigilância levadas a cabo pelos serviços secretos dos EUA, os quais recolhiam dados pessoais, de forma generalizada e indiscriminada, através da NSA[26]. *M. Schrems*, por considerar que as revelações de *Snowden* não poderiam ser ignoradas, apresentou queixa à autoridade de controlo de proteção de dados da Irlanda - *Data Protection Commissioner*. Neste sentido, *M. Schrems* pretendia obter a proibição destas transferências de dados pessoais e a investigação das práticas do *Facebook* quanto à recolha dos dados pessoais pelas autoridades dos EUA, na medida em que o direito e as práticas dos EUA não confeririam proteção suficiente aos cidadãos da UE, relativamente ao acesso de dados pessoais pelas autoridades públicas[27], incluindo a sua utilização em mecanismos de vigilância em massa

25 Tribunal de Justiça da União Europeia. Comunicado de Imprensa nº91/20 de 16 julho 2020 relativo ao Acórdão no processo C-311/18: 1.
26 Pires, M. Algumas considerações sobre a compatibilidade do sistema de Privacy Shield com o direito da União Europeia à luz do acórdão Schrems: 98.
27 Acórdão do Tribunal de Justiça, C-362/14, *Maximilian Schrems vs. Data Protection Commissioner*, de 6 de outubro de 2015.

desenvolvidos pela NSA, pelo FBI, entre outras entidades [28]. Contudo, o *Data Protection Commissioner* desconsiderou a queixa, alegando falta de fundamento, uma vez que os EUA, de acordo com os princípios do *Safe Harbor*, apresentariam um nível de proteção adequado. Discordando desta abordagem, *M. Schrems* recorreu ao Supremo Tribunal Irlandês, o qual considerou que, apesar de *Schrems* não ter colocado formalmente em causa a validade da Decisão *Safe Harbor*, a sua queixa denunciava, no fundo, a legalidade do regime instituído por essa decisão[29]. Neste sentido, o Supremo Tribunal Irlandês questionou o TJUE, via reenvio prejudicial, relativamente à validade da decisão de adequação do *Safe Harbor*, bem como se esta decisão invalidaria o prosseguimento de uma queixa individual, por parte das autoridades de controlo nacionais, quando existem suspeitas da utilização indevida de dados pessoais.

Esta queixa de *M. Schrems* acabou por levar o TJUE a invalidar a Decisão 2000/520, relativa ao nível de proteção assegurado pelos princípios do *Safe Harbor*, atendendo a que este mecanismo não vinculava as autoridades norte-americanas, prevalecendo o direito dos EUA em caso de conflito com os princípios de privacidade definidos[30]. Para tal, foi imperativo o TJUE esclarecer o significado de "nível de proteção adequado", num cenário pré-RGPD, face aos artigos da Carta dos Direitos Fundamentais da União Europeia, à recente jurisprudência e às normas europeias existentes sobre transferências de dados, tendo sido concluído que deveria ser entendido como "substancialmente equivalente" ao garantido pela União Europeia[31]. No seguimento da queixa, o TJUE esclareceu ainda que as autoridades nacionais de proteção de dados têm o dever de investigar queixas relacionadas com o tratamento de dados pessoais em países terceiros, mesmo quando já existe uma decisão de adequação *in place*.

Ainda na sequência do Acórdão *Schrems* I, o TJUE identificou alguns pontos fulcrais para que a *framework* para a proteção de dados no país terceiro seja equivalente à da UE, nomeadamente: eficácia da *framework*, ou seja, o país terceiro deve garantir a existência de instrumentos jurídicos para a proteção dos direitos fundamentais, que sejam

28 Pinheiro, A. Consequências do Acórdão Schrems II.
29Saugmandsgaard, H. Conclusões do Advogado-Geral Henrik Saugmandsgaard relativas ao Processo C-311/18.
30 Lopes, T. Responsabilidade e governação das empresas no âmbito do novo Regulamento sobre a Proteção de Dados: 50.
31 Acórdão do Tribunal de Justiça, C-362/14, *Maximilian Schrems vs. Data Protection Commissioner*, de 6 de outubro de 2015.

capacitados para responsabilizar e punir eventuais infratores; existência de meios de recurso judicial, disponíveis aos titulares, que garantam uma forma de reação efetiva contra as empresas que executam o tratamento de dados pessoais[32].

Naquele que foi o início do segundo episódio da saga, *M. Schrems* foi convidado a reformular a sua queixa, considerando a anulação do *Safe Harbor*. Nesta queixa, *M. Schrems* manteve a tese de que os EUA não assegurariam uma proteção eficaz dos dados transferidos e solicitou a suspensão ou proibição da transferência UE-EUA dos seus dados pessoais. A *Facebook Ireland*, entretanto, passou a transferir os dados tendo como base as cláusulas de proteção de dados presentes no anexo da Decisão 2010/87[33], relativa a cláusulas contratuais-tipo, as ditas *Standard Contractual Clauses* (SCC), aplicáveis à transferência de dados pessoais da UE para subcontratantes estabelecidos em países terceiros. A autoridade de controlo irlandesa, ao considerar que o tratamento da queixa de *M. Schrems* estaria dependente da validade da Decisão 2010/87, iniciou um processo para que o Supremo Tribunal Irlandês submetesse ao TJUE um pedido de decisão prejudicial[34]. De notar que, durante o período que sucedeu o início deste processo, a Comissão Europeia emitiu a Decisão 2016/1250, relativa ao nível de proteção assegurado pelo *Privacy Shield* UE-EUA, revogou a Diretiva 95/46, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, de 24 de outubro de 1995, a qual foi substituída pelo Regulamento (UE) 2016/679 e ainda emitiu a Decisão 2016/2297 que alterou as Decisões 2001/497 e 2010/87, relativas às cláusulas contratuais-tipo aplicáveis à transferência de dados pessoais para países terceiros.

O TJUE foi questionado quanto à aplicabilidade do RGPD nas transferências de dados pessoais com base nas cláusulas da Decisão 2010/87, quanto ao nível de exigência do RGPD, no que diz respeito à proteção de dados pessoais transferidos para países

32 Pires, M. Algumas considerações sobre a compatibilidade do sistema de Privacy Shield com o direito da União Europeia à luz do acórdão Schrems: 98.
33 Comissão europeia, Decisão de execução da Comissão número 2010/87, a cláusulas contratuais-tipo aplicáveis à transferência de dados pessoais para subcontratantes estabelecidos em países terceiros, nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho, conforme alterada pela Decisão de Execução (UE) 2016/2297 da Comissão, de 16 de dezembro de 2016.
34 Acórdão do Tribunal de Justiça, C-362/14, *Maximilian Schrems vs. Data Protection Commissioner*, de 6 de outubro de 2015.

terceiros e quanto às obrigações das autoridades de controlo neste contexto. Assim, surgiu a questão da validade tanto da Decisão 2010/87 como da Decisão 2016/1250.

O Tribunal de Justiça entendeu que o RGPD é aplicável a qualquer transferência de dados pessoais, no âmbito de uma atividade comercial, efetuada por um operador económico estabelecido num Estado-Membro para um outro operador estabelecido num país terceiro, independentemente de eventuais tratamentos posteriores a que os dados possam ser submetidos no país de destino, incluindo para efeitos de segurança pública, de defesa e de segurança do Estado pelas autoridades do país terceiro em causa[35]. Relativamente ao nível de proteção dos dados pessoais transferidos para países terceiros, importa referir que o artigo 46.º do RGPD "Transferências sujeitas a garantias adequadas", prevê que, no nº 1, se não tiver sido tomada uma decisão de adequação, os responsáveis pelo tratamento só podem transferir dados pessoais para um país terceiro "se tiverem apresentado garantias adequadas, e na condição de os titulares dos dados gozarem de direitos oponíveis e de medidas jurídicas corretivas eficazes" e que, de acordo com o nº 2 (alínea c), essas garantias podem resultar de "cláusulas-tipo de proteção" elaboradas pela Comissão. Em suma, o TJUE afirmou que os requisitos do RGPD sobre direitos oponíveis, garantias adequadas e medidas jurídicas eficazes devem ser aplicados de forma que os titulares, cujos dados são transferidos para um país terceiro com base em SCC, possam beneficiar de um nível de proteção equivalente ao assegurado na UE. Assim, o nível de proteção adequado deve ser avaliado tendo em conta as estipulações contratuais acordadas entre o exportador (UE) e o destinatário dos dados pessoais (país terceiro), bem como os elementos pertinentes do sistema jurídico do país terceiro em causa[36]. Por último, quanto às obrigações das autoridades de controlo, no contexto da transferência de dados pessoais para países terceiros, o TJUE declarou que, em conformidade com o artigo 58.º ("Poderes"), nº 2 do RGPD, interpretado em conjunto com o artigo 8.º ("Direito à proteção de dados pessoais"), da Carta dos Direitos Fundamentais da União Europeia, o respeito das exigências, que o direito fundamental à proteção de dados pessoais implica, está sujeito ao controlo de autoridades independentes, pelo que estas autoridades devem agir de forma a assegurar a correta aplicação deste regulamento. Portanto, a não ser que exista uma decisão de adequação adotada pela

35 Acórdão do Tribunal de Justiça, C-311/18, *Data Protection Commissioner vs. Facebook Ireland Ltd & Maximilian Schrems*, de 16 de julho de 2020.
36 Saugmandsgaard, H. Conclusões do Advogado-Geral Henrik Saugmandsgaard relativas ao Processo C-311/18.

Comissão, as autoridades de controlo estão incumbidas de suspender, ou até mesmo proibir, as transferências de dados para países terceiros sempre que considerarem que as SCC não são ou não podem ser respeitadas pelo país terceiro em causa e quando a proteção adequada dos dados transferidos, exigida pela UE, não pode ser assegurada por outros meios, no caso do próprio exportador não ter posto termo à transferência[37].

No decorrer deste processo, a validade da Decisão 2010/87 foi examinada, considerando a sua versão atual resultante da Decisão de Execução 2016/2297. De acordo com o TJUE, a sua validade não pode ser colocada em causa, uma vez que as SCC estabelecidas na Decisão não vinculam as autoridades do país terceiro por terem um caráter contratual. No entanto, a sua validade está inteiramente dependente da existência de mecanismos efetivos que garantam o respeito do nível de proteção adequado, exigido pelo direito da UE, e que possibilitem a suspensão/proibição da transferência de dados pessoais, com base nessas SCC, em caso de violação das mesmas ou na impossibilidade do seu cumprimento. O TJUE manifestou que esta Decisão prevê tais mecanismos, os quais advêm da imposição, tanto ao exportador como ao destinatário dos dados, de levar a cabo esta verificação prévia, bem como à obrigação do destinatário informar o exportador sempre que se verifique a impossibilidade de cumprir o estabelecido nas SCC, pertencendo ao exportador o dever da suspensão da transferência e/ou da rescisão do contrato[38].

Por último, a validade da Decisão 2016/1250, relativa ao nível de proteção assegurado pelo *Privacy Shield*, foi também alvo de investigação face aos requisitos do RGPD, lidos à luz das disposições da Carta dos Direitos Fundamentais da União Europeia. O TJUE pronunciou que, à semelhança da Decisão *Safe Harbor*, a Decisão *Privacy Shield* não estabelecia as garantias necessárias contra a ingerência das autoridades de informação norte-americanas no exercício dos direitos fundamentais dos titulares, cujos dados são transferidos para este país terceiro, relativos ao respeito da vida privada, à proteção dos dados pessoais e à proteção jurisdicional efetiva. Deste modo, a regulamentação interna dos EUA, no que diz respeito ao acesso e utilização dos dados pessoais provenientes da UE pelas autoridades públicas americanas, resulta numa grave

37 Saugmandsgaard, H. Conclusões do Advogado-Geral Henrik Saugmandsgaard relativas ao Processo C-311/18.
38 Tribunal de Justiça da União Europeia. Comunicado de Imprensa nº91/20 de 16 julho 2020 relativo ao Acórdão no processo C-311/18: 3.

fragilidade na proteção adequada dos dados e seus titulares, pelo que a exigência do nível de proteção "equivalente" ao garantido na UE não é satisfeita, na medida em que os programas de vigilância levados a cabo com base nessa regulamentação não são limitados ao estritamente necessário. Acrescentou ainda que a regulamentação interna dos EUA, apesar de incluir exigências para as autoridades americanas aquando da implementação dos ditos programas de *surveillance*, não confere aos titulares dos dados direitos oponíveis às autoridades americanas nos tribunais[39].

Ainda no que diz respeito à imposição de proteção jurisdicional, o TJUE declarou que o mecanismo de mediação previsto no *Privacy Shield*, contrariamente ao que a Comissão considerou aquando da sua decisão de adequação, não oferece aos titulares uma via de recurso num órgão que apresente garantias proporcionais às exigidas pelo direito da UE, as quais sejam capazes não só de assegurar a independência do mediador previsto, mas também a existência de normas que o habilitem a adotar decisões vinculativas para os serviços de informações americanos[40].

Considerando os motivos apresentados, o TJUE concluiu que, à luz da Carta dos Direitos Fundamentais da União Europeia, tendo por base os artigos 7.º, 8.º e 52.º (direito à vida privada, direito à proteção de dados pessoais e âmbito e interpretação dos direitos fundamentais, respetivamente), a validade da Decisão 2010/87 não é afetada, no entanto, declarou inválida a Decisão 2016/1250, uma vez que o *Privacy Shield*, à semelhança do *Safe Harbor*, consagrava o primado das exigências relativas à segurança nacional, ao interesse público e ao respeito da legislação americana, possibilitando assim ingerências nos direitos fundamentais dos cidadãos europeus, cujos dados são transferidos para os EUA[41].

39 Tribunal de Justiça da União Europeia. Comunicado de Imprensa nº91/20 de 16 julho 2020 relativo ao Acórdão no processo C-311/18.
40 Tribunal de Justiça da União Europeia. Comunicado de Imprensa nº91/20 de 16 julho 2020 relativo ao Acórdão no processo C-311/18.
41 Tribunal de Justiça da União Europeia. Comunicado de Imprensa nº91/20 de 16 julho 2020 relativo ao Acórdão no processo C-311/18.

### 3.2 Análise Crítica Geral

Atualmente, as empresas, independentemente do seu setor de atuação, seriam incapazes de fazer negócio ou participar no comércio internacional sem terem a capacidade de transferir dados além-fronteiras. O comércio global da UE está intimamente ligado ao fluxo transfronteiriço de dados, sendo as SCC o principal instrumento legal e o mecanismo mais amplamente utilizado para a transferência de dados pessoais para países terceiros, sendo, portanto, essenciais para a economia global[42].

A conclusão do TJUE relativamente à adequação das SCC para garantir contratualmente um nível de proteção equivalente dos dados transferidos para um país terceiro pretendeu, no fundo, não gerar um limbo jurídico. Esta decisão é, de certa forma, ambígua na medida em que a necessidade de garantir o cumprimento de medidas adequadas para proteger os dados pessoais, de acordo com os artigos 45.º ("Transferências com base numa decisão de adequação") e 46.º ("Transferências sujeitas a garantias adequadas") do RGPD, aplica-se tanto às decisões de adequação da Comissão Europeia como a cláusulas-tipo. Ora, se o *Privacy Shield* foi considerado inválido com base na incompatibilidade entre o direito da UE e a legislação de segurança norte-americana, seria expectável que as SCC estabelecidas para regular a transferência de dados precisamente para os EUA também teriam a mesma consequência jurídica. Portanto, perante este cenário, não é fácil compreender que as SCC não estejam também sujeitas a escrutínio por parte da Comissão, no que diz respeito à adequação da proteção oferecida na transferência de dados pessoais para um país terceiro, por não se dirigirem concretamente a um Estado, tendo o TJUE interpretado o RGPD de forma a atribuir às autoridades de controlo a competência desta verificação[43].

No fundo, o TJUE decidiu em conformidade com a jurisprudência dos últimos anos, a qual assenta numa posição firme a favor da proteção de dados pessoais, cabendo à lei governar a tecnologia e não o contrário, pelo que as empresas e outras partes interessadas devem encontrar soluções que permitam oferecer a proteção adequada dos dados pessoais exigida na UE[44]. Por exemplo, em 2017, o Tribunal emitiu o Parecer 1/15, projeto de

42 Digital Europe. An early analysis of Schrems II – key questions and possible ways forward.
43Pinheiro, A. Consequências do Acórdão Schrems II.
44 Christakis, T. "Schrems III"? First Thoughts on the EDPB post-Schrems II Recommendations on International Data Transfers (Part 1).

acordo entre o Canadá e a UE - transferência dos dados dos registos de identificação dos passageiros aéreos, no qual se opôs à entrada em vigor do Acórdão, insistindo no estabelecimento de regras rigorosas quanto à implementação concreta das leis de vigilância[45]. Em 2016, nos acórdãos *Tele2 Sverige* e *Tom Watson*, o Tribunal impôs limitações aos regimes de retenção de dados pessoais decididos pelos governos da UE e, em 2014, no Acórdão *Digital Rights Ireland*, o TJUE declarou inválida a Diretiva de retenção de dados[46].

Na Decisão *Schrems* II, o TJUE concluiu que, para as SCC serem válidas, os responsáveis pelo tratamento e os subcontratantes, em colaboração com o país destinatário dos dados pessoais, devem realizar uma avaliação da adequação do sistema jurídico do país terceiro, com base nos requisitos do artigo 45.º do RGPD e tendo em conta as circunstâncias específicas da transferência. Sempre que esta avaliação não demonstrar a garantia de uma proteção eficaz, em particular devido ao risco de acesso indevido dos dados pessoais por parte das autoridades públicas do país terceiro, o responsável pelo tratamento ou o subcontratante só poderão considerar as SCC aplicáveis às suas transferências de dados se existir a possibilidade de estas adotarem medidas adicionais que possam colmatar o risco de inadequação do país terceiro, reforçando, assim, a proteção dos dados transferidos[47]. Contudo, na ausência de uma decisão de adequação propriamente dita, a determinação sobre se uma lei de vigilância de um país terceiro satisfaz ou não as salvaguardas necessárias, no que diz respeito à proteção de dados pessoais está longe de ser simples, indo muito além das regulares diligências entre fornecedores e clientes.

A necessidade de realizar avaliações relativas à adequação dos países terceiros, caso a caso, além de representar um encargo adicional para os responsáveis pelo tratamento e respetivos subcontratantes, os quais muitas vezes são empresas com recursos limitados, sendo cerca de 65% PME's ou *startups*[48], a autoridade e o dever destes decidirem sobre

45 Parecer do Tribunal de Justiça 1/15 de 26 de julho de 2017, Projeto de acordo entre o Canadá e a União Europeia.
46 Christakis, T. "Schrems III"? First Thoughts on the EDPB post-Schrems II Recommendations on International Data Transfers (Part 1).
47 Acórdão do Tribunal de Justiça, C-311/18, *Data Protection Commissioner vs. Facebook Ireland Ltd & Maximilian Schrems*, de 16 de julho de 2020.
48 Moniz, G. Schrems II – a saga da proteção de dados pessoais continua.

a adequação dos regimes de segurança nacional de outros países é, no mínimo, discutível por não ser uma tarefa tipicamente esperada de empresas privadas.

Outra questão que se coloca, no que diz respeito às avaliações exigidas da adequação do sistema jurídico do país terceiro, prende-se com a possibilidade de existirem avaliações diferentes entre empresas, originando soluções contraditórias relativamente às SCC, as quais apenas poderiam ser resolvidas pelas autoridades de controlo, que, por sua vez, também poderiam apresentar avaliações contraditórias, sendo necessária uma interpretação uniforme entre as autoridades de controlo nacionais da UE[49].

A 11 de novembro de 2020, a *European Data Protection Board* (EDPB) emitiu a Recomendação 1/2020, relativamente às medidas adicionais para complementar as ferramentas de transferência de dados pessoais, incluindo as SCC, de forma a garantir *compliance* com o nível de proteção exigida na UE. Nesta recomendação, a qual foi emitida precisamente na sequência da Decisão *Schrems* II, a EDPB aconselha as empresas exportadoras de dados, em primeiro lugar, a conhecer bem as suas transferências, estando cientes de onde circulam os dados e da adequação e relevância dos mesmos, em relação ao propósito pelo qual são transferidos e processados no país terceiro, seguindo-se um *roadmap*, dirigido às empresas, para aplicação do princípio da responsabilidade nas transferências de dados pessoais, incluindo recomendações para a verificação da adequação da ferramenta de transferência em uso, para a avaliação da proteção assegurada no país terceiro e para a adoção de medidas suplementares[50]. Ao ler as recomendações relativas à adoção de medidas suplementares, ficamos com a sensação de que qualquer transferência de dados pessoais da UE para países terceiros que não beneficiem de uma decisão de adequação da Comissão, será difícil. A EDPB, no Anexo 2, fornece uma lista não exaustiva de tais medidas, incluindo medidas técnicas, contratuais e organizativas, e afirma que, nos casos em que nenhuma medida suplementar possa corrigir as deficiências identificadas, as transferências deverão ser interrompidas. No que diz respeito às medidas técnicas, a encriptação dos dados pessoais é a medida a destacar pela EDPB como a principal técnica para exportar dados de forma segura (uma vez que impossibilita o acesso aos dados propriamente ditos no país destinatário), sobre a qual são feitas várias

49 Digital Europe. An early analysis of Schrems II – key questions and possible ways forward.
50 EDPB. Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.

recomendações relativas à sua aplicação, incluindo a necessidade de encriptação antes da transferência de dados, a resiliência da encriptação obrigatória face à criptanálise pelas autoridades públicas dos países terceiros, a implementação impecável do algoritmo de encriptação em si, a imposição de manter as chaves de encriptação na UE, entre outras[51]. Portanto, após as empresas terem conduzido as avaliações da adequação do sistema jurídico do país terceiro e implementado as medidas suplementares imprescindíveis à transferência de dados pessoais, sempre que tal seja possível, ainda têm que documentar este processo e submeter o pedido de autorização, sempre que exigido pelo mecanismo de transferência escolhido e reavaliar a sua abordagem regularmente. Claramente, a orientação emitida pela EDPB é complexa, representando um enorme desafio para as empresas da UE, as quais estão perante uma tarefa quase impossível - encontrar soluções que permitam manter o padrão de proteção de dados da UE, independentemente do país destinatário, num mundo global em que os direitos, as leis e as normas divergem consideravelmente[52].

51 EDPB. Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.
52 Fennessy, C. A breakdown of EDPB's recommendations for data transfers post-'Schrems II'.

## 4. Reflexões Finais

O Acórdão proferido pelo TJUE (C-311/18, "*Schrems* II") veio consolidar a importância de manter um nível de proteção elevado no que concerne aos dados pessoais transferidos da UE para países terceiros, abordando, de forma genérica, a questão do acesso a dados pessoais pelo governo e autoridades públicas por parte de qualquer país terceiro. Na verdade, a decisão do caso *Schrems* II vai bastante além do *Schrems* I, na medida em que o primeiro episódio apenas invalida os princípios de privacidade do *Safe Harbor*, para a transferência de dados UE-EUA, enquanto que no *Schrems* II, além da decisão de adequação *Privacy Shield* UE-EUA ter sido invalidada, o TJUE insistiu que todos os intervenientes relevantes devem assegurar que o *standard* para a proteção de dados pessoais da UE é mantido e aplicado quando se recorre a outros meios legais para a transferência de dados, que não decisões de adequação.

Com o caso *Schrems* II fica claro que as SCC são atualmente a alternativa a considerar no que diz respeito à transferência de dados pessoais para os países que não beneficiem de uma decisão de adequação, pelo que as empresas devem focar-se no estabelecimento de SCC personalizadas, as quais garantam a manutenção do nível de proteção dos dados pessoais assegurada pelo RGPD aquando da sua transferência para um país terceiro, não se limitando, portanto, a utilizar um *template* contratual. No entanto, uma garantia contratual não deixa de ser insuficiente se a lei do país terceiro exigir ou permitir o acesso a dados pessoais em contradição com os requisitos do RGPD. Deste modo, os Responsáveis pelo Tratamento, sob o controlo das Autoridades de Proteção de Dados, ficam incumbidos de assegurar a eficácia das SCC na prática, o que, por si só, representa um desafio considerável para as empresas, as quais têm de levar a cabo *a priori* uma avaliação para determinar se o país terceiro oferece ou não garantias legais equivalentes às da UE. Escusado será dizer que esta avaliação pode terminar com as transferências de dados para um número importante de Estados, nomeadamente a China e a Rússia, cujos sistemas jurídicos oferecem substancialmente menos garantias do que os EUA em relação ao acesso dos dados por autoridades públicas e governamentais.

Assim, este Acórdão trouxe várias incertezas quanto à base jurídica para as transferências internacionais de dados pessoais, incluindo inseguranças relativas à perspetiva de uma versão 3.0 da decisão de adequação *Safe Harbor*, para além de também levantar questões relativamente às decisões de adequação em vigor com outros países terceiros.

Em adição, veio ainda revelar algumas inseguranças relacionadas com a avaliação dos países terceiros quanto à garantia de proteção adequada dos dados pessoais e seus titulares, uma vez que, até à data do Acórdão, a responsabilidade desta avaliação era centralizada na Comissão Europeia, tendo havido uma viragem para a descentralização desta autoridade no sentido de colocar este processo sob o controlo das autoridades nacionais competentes. Ora, se a própria Comissão Europeia com todo o seu conhecimento e recursos ao dispor, provou estar errada duas vezes consecutivas em relação a tais avaliações (*Safe Harbor* e *Privacy Shield*), coloca-se a questão pertinente de como poderiam as empresas da UE ter um melhor desempenho nesta tarefa.

O estabelecimento de uma regulação transfronteiriça para a proteção de dados pessoais é um processo bastante complexo pela necessidade de satisfazer, por um lado, a preocupação de salvaguardar a liberdade do desenvolvimento empresarial e, simultaneamente, garantir um nível de proteção adequado dos dados pessoais e seus titulares, e, por outro, assegurar a proteção da segurança nacional e ainda manter uma relação diplomática e comercial com os países terceiros, especialmente com aqueles que são as grandes potências internacionais.

Não existindo uma solução ideal, as decisões de adequação da Comissão Europeia, durante vários anos, foram a principal base legal para a transferência de dados além-fronteiras, no entanto, a postura exigente do TJUE vem insistir na afirmação efetiva do direito fundamental à proteção de dados. Poder-se-ia esperar que o *Schrems* II surtisse o efeito desejado de promover a convergência dos *standards* de proteção de dados a nível internacional, como forma de facilitar o fluxo de dados e, consequentemente, o comércio. Esta saga jurisprudencial gerou pressão nos países terceiros, por verem o tráfico de dados dificultado, estando a UE a tentar, de certa forma, afirmar-se como um "regulador" para a transferência de dados pessoais a nível internacional. Outro dado importante, será observar como as autoridades de controlo nacionais irão agir perante este Acórdão quando ainda não houve tempo suficiente para se tirar conclusões definitivas. O tema da proteção

de dados está longe de estar esgotado e a divergência do entendimento relativo à privacidade é tão vincado que garantir um nível de proteção eficaz, independentemente do local para onde os dados pessoais viajam, constitui um enorme desafio sem solução definitiva num horizonte próximo.

## Bibliografia


Acórdão do Tribunal de Justiça, C-362/14, *Maximilian Schrems vs. Data Protection Commissioner*, de 6 de outubro de 2015. [Online]. Disponível em: http://curia.europa.eu/juris/document/document.jsf?docid=169195&doclang=pt [Consultado a 08/11/2020].

Acórdão do Tribunal de Justiça, C-311/18, *Data Protection Commissioner vs. Facebook Ireland Ltd & Maximilian Schrems*, de 16 de julho de 2020. [Online]. Disponível em: http://curia.europa.eu/juris/document/document.jsf;jsessionid=B7696A55E724D9CD6BAC0B89552911FD?text=&docid=228677&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=13263774 [Consultado a 15/11/2020].

American Arbitration Association. ICDR-AAA EU-U.S. and/or Swiss-U.S. Privacy Shield Arbitral Fund Contributions. [Online]. Disponível em: https://go.adr.org/privacyshieldfund.html [Consultado a 01/11/2020].

Autoridade europeia para a Proteção de Dados. Opinion 4/2016 on the EU-U.S. Privacy Shield draft adequacy decision, de 30 de maio de 2016. [Online]. Disponível em: https://edps.europa.eu/sites/edp/files/publication/16-05-30_privacy_shield_en.pdf [Consultado a 01/11/2020].

Christakis, T. 2020. "Schrems III"? First Thoughts on the EDPB post-Schrems II Recommendations on International Data Transfers (Part 1). [Online]. Disponível em: https://europeanlawblog.eu/2020/11/13/schrems-iii-first-thoughts-on-the-edpb-post-schrems-ii-recommendations-on-international-data-transfers-part-1/ [Consultado a 22/11/2020].

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, p. 3. [Online] Disponível em: http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52013DC0847&qid=1488287495250&from=PT> [Consultado a 10/11/2020].

Comissão europeia, “Decisão 2000/520 relativa ao nível de proteção assegurado pelos princípios de ‘porto seguro’ e pelas questões e pelas respectivas FAQ emitidas pelo Department of Commerce dos Estados Unidos da América”, de 26 de julho de 2000. [Online]. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32000D0520&from=PT [Consultado a 10/11/2020].

Comissão europeia, “Decisão de execução da Comissão número 2010/87, a cláusulas contratuais-tipo aplicáveis à transferência de dados pessoais para subcontratantes estabelecidos em países terceiros, nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho”, de 5 de fevereiro de 2010. [Online]. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32010D0087&from=PT Consultado a 13/11/2020].

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. 3-6. [Online]. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016D1250&from=PT. [Consultado a 05/11/2020].

Comissão europeia, “Decisão da Comissão nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho e relativa ao nível de proteção assegurado pelos princípios de “porto seguro” e pelas respetivas questões mais frequentes (FAQ) emitidos pelo Department of Commerce dos Estados Unidos da América”, de 26 de julho de 2000. [Online]. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32000D0520&from=PT [Consultado a 15/11/2020].

Comissão Nacional de Proteção de Dados, Parecer n.º 14/2000 [Online]. Disponível em: https://www.cnpd.pt/home/decisoes/2000/htm/par/par014-00.htm [Consultado a 15/11/2020].

Comissão Nacional de Proteção de Dados, Parecer n.º 17/2000 [Online]. Disponível em: https://www.cnpd.pt/home/decisoes/2000/htm/par/par017-00.htm [Consultado a 15/11/2020].

Digital Europe. 2020. An early analysis of Schrems II – key questions and possible ways forward [Online]. Disponível em: https://www.digitaleurope.org/resources/an-early-analysis-of-schrems-ii-key-questions-and-possible-ways-forward/ [Consultado a 21/11/2020].

EDPB. 2020. Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, adopted on 10 November 2020. [Online]. Disponível em: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf [Consultado a 22/11/2020].

Fennessy, C. 2020. A breakdown of EDPB's recommendations for data transfers post-'Schrems II'. [Online]. Disponível em: https://iapp.org/news/a/a-break-down-of-edpbs-recommendations-for-data-transfers-post-schrems-ii/ [Consultado a 22/11/2020].

Governo do Brasil - Ministério da Defesa. 2020. Lei Geral de Proteção de Dados – LGPD [Online]. Disponível em: https://www.gov.br/defesa/pt-br/acesso-a-informacao/lei-geral-de-protecao-de-dados-pessoais-lgpd [Consultado a 31/10/2020].

Jesus, I. 2018. 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? *In* Anuário da Proteção de Dados 2018. [Online]. Disponível em: http://cedis.fd.unl.pt/wp-content/uploads/2018/04/ANUARIO-2018-Eletronico.pdf [Consultado a 05/11/2020].

Lopes, T. 2018. Responsabilidade e governação das empresas no âmbito do novo Regulamento sobre a Proteção de Dados: 50. *In* Anuário da Proteção de Dados 2018. [Online]. Disponível em: http://cedis.fd.unl.pt/wp-content/uploads/2018/04/ANUARIO-2018-Eletronico.pdf [Consultado a 10/11/2020].

Moniz, G. 2020. Schrems II – a saga da proteção de dados pessoais continua. *In* Observador [Online]. Disponível em: https://observador.pt/opiniao/schrems-ii-a-saga-da-protecao-de-dados-pessoais-continua/ [Consultado a 21/11/2020].

Okwara, E. 2020. Kenya takes important step toward in data protection. [Online]. Disponível em: https://iapp.org/news/a/kenya-takes-important-step-forward-in-data-protection/ [Consultado a 31/10/2020].

Parecer do Tribunal de Justiça 1/15 de 26 de julho de 2017, Projeto de acordo entre o Canadá e a União Europeia - Transferência dos dados dos registos de identificação dos passageiros aéreos da União para o Canadá. [Online]. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:62015CG0001&from=IT [Consultado a 22/11/2020].

Pinheiro, A. 2020. Consequências do Acórdão Schrems II. [Online]. Disponível em: https://asousapinheiro.com/2020/08/21/consequencias-do-acordao-schrems-ii/ [Consultado a 14/11/2020].

Pires, M. 2018. Algumas considerações sobre a compatibilidade do sistema de *Privacy Shield* com o direito da União Europeia à luz do acórdão Schrems. *In* Anuário da Proteção de Dados 2018. [Online]. Disponível em: http://cedis.fd.unl.pt/wp-content/uploads/2018/04/ANUARIO-2018-Eletronico.pdf [Consultado a 05/11/2020].

Privacy Shield Framework. How to join Privacy shield (part 1). [Online]. Disponível em: https://www.privacyshield.gov/article?id=How-to-Join-Privacy-Shield-part-1 [Consultado a 01/11/2020].

Privacy Shield Framework. Privacy Shield Program Overview. [Online]. Disponível em: https://www.privacyshield.gov/Program-Overview [Consultado a 01/11/2020].

Privacy Shield Framework. A Step-by-Step Guide to Self-Certification on the Privacy Shield Website. [Online]. Disponível em: https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t000000079DJ [Consultado a 01/11/2020].

Privacy Shield Framework. 7. Verification. [Online]. Disponível em: https://www.privacyshield.gov/article?id=7-Verification [Consultado a 08/11/2020].

Raposo, Sá Miranda & Associados. 2015. *Safe Harbor*: Perguntas e Respostas. [Online]. Disponível em:

https://www.pra.pt/site/assets/files/1222/safe_harbor_nota_informativa.pdf [Consultado a 15/11/2020].

Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). [Online]. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT [Consultado a 31/10/2020].

Saugmandsgaard, H. Conclusões do Advogado-Geral Henrik Saugmandsgaard relativas ao Processo C-311/18. [Online]. Disponível em: http://curia.europa.eu/juris/document/document.jsf;jsessionid=B7696A55E724D9CD6BAC0B89552911FD?text=&docid=221826&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=13263774 [Consultado a 15/11/2020].

Tribunal de Justiça da União Europeia. Comunicado de Imprensa nº91/20 de 16 julho 2020 relativo ao Acórdão no processo C-311/18. [Online]. Disponível em: https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091pt.pdf [Consultado a 08/11/2020].

U.S. Department of Commerce. EU-U.S. Privacy Shield Framework Principles. [Online]. Disponível em: https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004qAg [Consultado a 01/11/2020].