What´s in a Name?
Uma Breve Análise do Nível de Protecção Adequado no Âmbito das Transferências de Dados Pessoais dos Cidadãos da União Europeia para Países Terceiros

Ricardo Rodrigues de Oliveira*

Resumo: O presente texto pretende questionar o efeito útil aparentemente decorrente do desenvolvimento pelo legislador europeu das cláusulas relativas ao nível de protecção para as transferências de dados pessoais de cidadãos da União Europeia para países terceiros. A Directiva 95/46/CE foi substituída pelo Regulamento (UE) 2016/679, assim se mudando, em parte, o paradigma anterior, visto que este é mais desenvolvido no que respeita aos critérios para a tomada de decisões pela Comissão. No entanto, deveria era ter sido modificada a política de negociações, especialmente com os EUA, para garantir uma protecção efectiva, tanto *de iure* como de facto.

Palavras-chave: *Directiva 95/46/CE; Nível de Protecção Adequado; Regulamento (UE) 2016/679; Schrems.*

Abstract: The present text aims at questioning the 'effet utile' apparently resulting from the development by the European legislator of the clauses relative to the level of protection for the transference of EU citizens' personal data to third countries. The Directive 95/46/EC was replaced by the Regulation (EU) 2016/679, thus partially changing the previous paradigm, as the latter is more developed regarding the decision-making criteria by the Commission. However, the negotiating policy is what should have been modified, especially with the USA, to guarantee an effective protection, both de iure as de facto.

Keyword: *Adequate Level of Protection; Directive 95/46/EC; Regulation (EU) 2016/679; Schrems.*

---

* Doutorando no Instituto Universitário Europeu (EUI), Investigador do Centro de Investigação em Direito Público da Faculdade de Direito da Universidade de Lisboa (FDUL) e Investigador da Jurisnova da Faculdade de Direito da Universidade Nova de Lisboa (FDUNL).

Introdução

A relação dos cidadãos e dos poderes públicos com a transferência e processamento de dados pessoais, bem como a sua protecção, está a mudar rapidamente no mundo electronicamente globalizado dos tempos contemporâneos. São cada vez mais os estudos[1] e a literatura que atestam as diferentes exigências que rodeiam as deslocações de informação dos cidadãos, tanto intra como inter-jurisdições. Eles revelam uma tensão crescente entre os direitos à privacidade e à intimidade[2] e as potenciais utilizações que a compilação de dados em grandes quantidades oferece.

Desde a criação mais básica de perfis comerciais até ao complexo entrecruzamento de dados de geolocalização para efeitos de investigação criminal ou de contra-terrorismo, há uma rede global de entidades e plataformas, privadas, públicas e sob regimes mistos de cooperação e interoperabilidade, que gerem bases de dados com dimensões, as mais das vezes, verdadeiramente *orwellianas*. A nível europeu, as instituições, com a Comissão à cabeça, têm vindo a desempenhar um papel cada vez mais activo, em conjunto com os Estados-Membros, na cumplicidade administrativa de, por um lado, recorrer à compilação massiva de dados que permitem identificar os indivíduos e localizá-los geográfica e temporalmente, para os mais diversos fins, e, por outro, tentar limitar a disseminação, acesso e consequente usos abusivos destes elementos.

A situação torna-se mais melindrosa quando os dados correm o risco de serem vertidos para meios de comunicação e espaços de armazenamento que não garantem uma isenção e garantias de protecção contra utilizações distintas daquelas consentidas originalmente pelos titulares dos dados. Com as aberturas permitidas pela internet das coisas, a certeza e segurança jurídicas do resguardo das informações só podem ser mantidas em condições relativamente estritas. Nomeadamente, com as garantias de que os controladores e administradores de sistemas não as libertem; de que não

---

[1] V. a título ilustrativo, a página electrónica da Comissão Europeia sobre os estudos mais recentes relativos à protecção de dados, bem como os diversos documentos e ligações acessíveis a partir desta plataforma. Disponível em: <http://ec.europa.eu/justice/data-protection/document/studies/index_en.htm> (acedido a 29/07/2017).

[2] V. Herrán Ortiz, Ana. "El derecho a la protección de datos personales en la sociedad de la información", *Cuadernos Deusto de Derechos Humanos*, n.º 26, 2003, pp. 9-92.

haja entidades a imiscuir livremente nas bases de dados, mesmo se forem autoridades públicas; e de que existam meios processuais ao alcance dos particulares para defesa dos seus interesses, direitos e liberdades, a par de um conjunto efectivo de sanções.

O tema desta investigação recai, precisamente, sobre um aspecto da actualidade da transmissão de dados no âmbito das relações externas da UE. Desde 1995, que o legislador europeu tem baseado a transferência de dados dos cidadãos do espaço eurocomunitário para o exterior em decisões de adequação, a determinar pela Comissão em cooperação com os Estados-Membros. Mediante negociações bilaterais, a instituição tem vindo a declarar que determinadas jurisdições externas apresentam garantias suficientes nos seus ordenamentos para que sejam consideradas como destinos 'seguros', facilitando o desenvolvimento das relações comerciais.

O presente trabalho é uma excursão simplificada pelo conceito de nível de protecção adequado na legislação eurocomunitária relativamente às transferências transnacionais de dados pessoais, *i.e.*, envio de informações dos cidadãos da União para bases de dados localizadas em países terceiros. O objectivo que subjaz é evidenciar a falta de proposição normativa a definir o conceito na evolução legislativa, deixando em aberto potenciais conclusões a este respeito, e, de outro tanto, demonstrar a prática negocial da Comissão nos acordos "porto seguro" e "escudo de protecção" estabelecidos com os EUA quanto a este assunto.

A inexistência de um conceito formalizado e alguma 'nebulosidade' dos trechos legais poderão explicar, em parte, a insuficiente investigação que a instituição insiste em levar a cabo de cada vez que dialoga com os EUA, preferindo confiar, sem exercício de eficaz ou notório contraditório, nas cartas e declarações de princípios que representantes institucionais de alguns sectores de actividade enviam para a Europa. A escolha deste exemplo deve-se a um conjunto de razões, como a importância norte-americana nas relações políticas, comerciais e económicas europeias com o exterior; a maior publicidade dos documentos negociais; a especificidade dos acordos UE-EUA por oposição aos demais países; e a toda a celeuma decorrente do caso *Wikileaks*.

Aparte esta introdução e as notas conclusivas, o artigo está dividido em 4 secções. A primeira e a terceira, mais breves, dão conta dos enunciados legais de 1995 e de 2016, focando-se na consagração do conceito de nível de protecção adequado, muito embora somente o primeiro informe

actualmente os procedimentos de adequação. A segunda e a quarta, mais extensas, debruçam-se sobre a insuficiente atenção executiva dada ao conceito, quer na primeira decisão de adequação da Comissão, designada por "porto seguro", e no desenvolvimento posterior no caso *Schrems*, quer na segunda decisão, mais recente e aprovada no âmbito da renovação legislativa europeia em matéria de protecção de dados, designada por "escudo de protecção de privacidade".

1. A Directiva 95/46/CE

A Directiva 95/46/CE de 24 de Outubro de 1995[3] criou, pela primeira vez, um regime relativo à transferência de dados pessoais dos cidadãos das Comunidades Europeias para países terceiros. Nos termos do n.º 1 do art. 25.º, os Estados-Membros deveriam cuidar que as transferências só fossem concretizadas para países que assegurassem um nível de protecção adequado relativamente ao tratamento e manutenção destas informações.

O legislador europeu não definiu o que deveria ser entendido por este patamar de adequação em 1995[4-5], tal como não o vai fazer em 2016. Apenas

---

[3] Directiva 95/46/CE do Parlamento Europeu e do Conselho de 24 de Outubro de 1995 relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (JO L 281/31, 23.11.1995). Tal como o actual pacote legislativo relativo à protecção de dados, a Directiva demorou algum tempo a ser elaborada e aprovada pelo seu cariz inovador e pela complexidade técnica. Este documento resulta de uma proposta da Comissão apresentada a 27 de Julho de 1990 e que depois foi adaptada pelo Conselho (COM (90) 314 final — SYN 287, 90/C 277/03), e alterada subsequentemente (92/C 311/04, 27.11.1992).

[4] Sendo que tal vai gerar diferentes preocupações de ambos os lados do Atlântico quanto ao que poderá significar, visto que os EUA nunca acabaram por importar verdadeiramente o conceito, segundo Estadella-Yuste, Olga. *La protección de la intimidad frente a la transmisión internacional de datos personales*. Madrid: Tecnos, 1995, p. 117. Para uma perspectiva norte-americana do problema da EU como uma *norm-giver* que pode cair na tentação da 'estandardização' das normas aplicáveis fora do seu território, v. Goldsmith, Jack e Wu, Tim. *Who controls the Internet? Illusions of a borderless world*. Oxford: Oxford University Press, 2006, pp. 173 e ss.

[5] Aliás, Herrán Ortiz, Ana. "El derecho a la protección de datos personales en la sociedad de la información", cit., p. 40, reflecte, ironicamente, que mais parece que se deve estabelecer qual o nível desadequado para se saber mais facilmente se o país terceiro oferece garantias suficientes para a transmissão de dados. Aquele seria o patamar abaixo do qual

referiu os critérios segundo os quais o nível de protecção teria de ser apreciado. Segundo o n.º 2, deveriam ser tidas em conta todas as circunstâncias relativas às transferências, singular ou colectivamente consideradas, nomeadamente "a natureza dos dados, a finalidade e a duração do tratamento ou tratamentos projectados, os países de origem e de destino final, as regras de direito, gerais ou sectoriais, em vigor no país terceiro em causa, bem como as regras profissionais e as medidas de segurança que são respeitadas nesse país".

Esta situação de indefinição do conceito levou a que o trecho fosse criticado por ambíguo[6] e por se assemelhar a outras disposições legais[7], criando alguma incerteza jurídica. Donde, não parece ser de partilhar a 'leveza' com que certa doutrina encara a regra como um conceito jurídico indeterminado, uma norma em branco, que, pela sua flexibilidade, se ajusta excepcionalmente bem ao colorido de situações às quais se aplica o seu modelo de estandardização[8].

À luz do n.º 6 do art. 25.º desta Directiva, caberia à Comissão constatar, segundo o procedimento de comitologia previsto nos termos do n.º 2 do art. 31.º, que países assegurariam esse tal *standard* de protecção adequado, tanto pela primeira vez como no caso de algum país que tivesse deixado de assegurar este limiar e a 'confiança' tivesse que ser reposta após negociações com os decisores europeus. A instituição apreciava, com base neste amplo critério e de forma casuística[9], como o vai fazer em 2016, a presença dos

---

ainda se produziriam efeitos negativos para os interessados quanto à protecção dos seus dados pessoais.

[6] Cerda Silva, Alberto. "El «nivel adecuado de protección» para las transferencias internacionales de datos personales desde la Unión Europea", *Revista de Derecho de la Pontificia Universidad Católica de Valparaíso*, n.º XXXVI, 2011, p. 335.

[7] Como, por exemplo, a expressão "protecção equivalente" da alínea a) do n.º 3 do art. 12.º da Convenção 108 do Conselho da Europa, de 28 de Janeiro de 1981, para a protecção dos indivíduos relativamente ao tratamento automatizado dos dados de carácter pessoal, ou a locução "garantias comparáveis" da Organização das Nações Unidas, *Guidelines for the Regulation of Computerized Personal Data Files*, A/RES/45/95, de 14 de Dezembro de 1990 (68.ª sessão plenária), para. 9.

[8] Heredero Higueras, Manuel. *La Directiva comunitaria de protección de datos de carácter personal*. Madrid: Aranzadi, 1997, p. 188.

[9] Cerda Silva, Alberto. "El «nivel adecuado de protección» para las transferencias internacionales de datos personales desde la Unión Europea", cit., p. 336.

mencionados critérios "em virtude da sua legislação interna ou dos seus compromissos internacionais", sempre no sentido de acautelar a protecção do direito à vida privada e dos direitos e liberdades fundamentais dos cidadãos[10].

Foram muito poucos (e, na maioria dos casos, pouco relevantes) os países a gozar de uma decisão de adequação. Contam-se Andorra[11], a Argentina[12], o Canadá (mas somente no que respeita as suas organizações comerciais)[13], as Ilhas Faroé[14], Guernsey[15], Israel[16], a Ilha de

---

[10] Importa mencionar que alguns documentos não legislativos ajudaram a compreender a leitura que deveria ser feita do nível de adequação pela falta de definição expressa. Através da flexibilização dos critérios interpretativos, tem sido possível, no entender de algumas entidades, contornar a inexistência de uma consagração cristalizada do conceito e adaptar as normas europeias às realidades externas para se determinar, como mencionado, de forma *ad hoc*, se dado país assegura o referido nível. Entre alguns destes textos, contam-se: *G29, First orientations on transfers of personal data to third countries – Possible ways forward in assessing adequacy*, XV D/5020/97-EN final WP4, de 26 de Junho de 1997. Disponível em: <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1997/wp4_en.pdf> (acedido a 3/12/2017), ou G29, *Working document. Transfers of personal data to third countries: Applying articles 25 and 26 of the EU Data Protection Directive*, DG XV D/5025/98 WP 12, de 24 de Julho de 1998. Disponível em: <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12_en.pdf> (acedido a 7/12/2017).

[11] Decisão da Comissão de 19 de Outubro de 2010 nos termos da Directiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de protecção de dados pessoais em Andorra (JO L 277, 21.10.2010).

[12] Decisão da Comissão de 30 de Junho de 2003 nos termos da Directiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de protecção de dados pessoais na Argentina (JO L 168, 05.7.2003).

[13] Decisão da Comissão de 20 de Dezembro de 2001 nos termos da Directiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de protecção proporcionado pela lei canadiana sobre dados pessoais e documentos electrónicos (*Personal Information and Electronic Documents Act*) (JO L 2, 4.1.2002).

[14] Decisão da Comissão de 5 de Março de 2010 nos termos da Directiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de protecção assegurado pela Lei sobre o tratamento de dados pessoais das Ilhas Faroé (JO L 58, 9.3.2010).

[15] Decisão da Comissão de 21 de Novembro de 2003 nos termos da Directiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de protecção de dados pessoais em Guernsey (JO L 308, 25.11.2003).

[16] Decisão da Comissão de 31 de Janeiro de 2011 nos termos da Directiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de protecção de dados pessoais pelo Estado de Israel no que se refere ao tratamento automatizado de dados (JO L 27, 1.2.2011).

Man[17], Jersey[18], a Nova Zelândia[19], a Suíça[20] e o Uruguai[21]. Nas diversas decisões, o legislador comunitário apenas decidia que a jurisdição assegurava um nível de protecção adequado, sem explorar o conceito.

2. A Decisão 2000/520/CE e o caso *Schrems*

Para além destes países, também os EUA gozaram de uma decisão a considerar o país como adequado para receber os dados pessoais dos cidadãos das Comunidades, embora através de um sistema algo diferente dos demais[22]. Pela sua importância económica e capacidade de diálogo político, os EUA conseguiram uma posição negocial de vantagem, baseada em compromissos, princípios gerais e questões mais frequentes[23]. É, sem dúvida, o país sobre cujos documentos de negociação mais se conhece publicamente, mas, precisamente por isso, é também a chave para compreender como é

---

[17] Decisão da Comissão de 28 de Abril de 2004 relativa à adequação do nível de protecção de dados pessoais na Ilha de Man (JO L 151, 30.4.2003).

[18] Decisão da Comissão de 8 de Maio de 2008 nos termos da Directiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de protecção de dados pessoais em Jersey (JO L 138, 28.5.2008).

[19] Decisão da Comissão de 19 de Dezembro de 2012 nos termos da Directiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de protecção de dados pessoais pela Nova Zelândia (JO L 28, 30.1.2013).

[20] Decisão da Comissão de 26 de Julho de 2000 nos termos da Directiva 95/46/CE do Parlamento Europeu e do Conselho e relativa ao nível de protecção adequado dos dados pessoais na Suíça (JO L 215, 25.8.2000).

[21] Decisão de execução da Comissão de 21 de Agosto de 2012 nos termos da Directiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de protecção de dados pessoais pela República Oriental do Uruguai no que se refere ao tratamento automatizado de dados (JO L 227, 23.08.2012).

[22] Decisão 2000/520/CE da Comissão de 26 de Julho de 2000 nos termos da Directiva 95/46/CE do Parlamento Europeu e do Conselho e relativa ao nível de protecção assegurado pelos princípios de «porto seguro» e pelas respectivas questões mais frequentes (FAQ) emitidos pelo *Department of Commerce* dos Estados Unidos da América (JO L 215 de 25.08. 2000).

[23] Levando a uma consequente tendência de aproximação das legislações europeia e norte-americana, nas palavras 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 qe nos dizem respeito?", publicado neste Anuário.

que deverá ter sido levada a cabo a 'investigação' que a Comissão fez para verificar o nível de adequação.

Logo no art. 1.º da Decisão 2000/520/CE, se percebe que a constatação das circunstâncias relativas às transferências de dados feita pela Comissão da legislação interna e dos compromissos internacionais dos EUA se baseou não numa indagação de facto, mas no recebimento de documentos com promessas de natureza política e princípios de aplicabilidade comercial e na consequente expectativa europeia de que todas as instituições norte-americanas, dentro ou fora do sector, os cumprissem. Sem haver qualquer definição do que seja o nível adequado, nos termos do n.º 1 do art. 1.º, a protecção proporcionada aos dados pessoais dos europeus derivava dos princípios da privacidade em "porto seguro" e das linhas de orientação publicadas pelo DOC, a 21 de Julho de 2000[24], segundo os 'compromissos' assumidos em 4 documentos anexos à Decisão: um memorando a explicar a autoridade e funções da FTC; um outro com uma clarificação sumária da legislação norte-americana quanto a danos por violação das regras de protecção da vida privada e autorizações explícitas no que respeita ao uso de informações pessoais de forma contrária aos princípios de "porto seguro"; uma carta de Robert Pitofsky, da FTC, dirigida a John Mogg, Diretor-geral do Mercado Interno da Comissão, respondendo às dúvidas deste relativamente à jurisdição da FTC sobre "protecção da vida privada na área das comunicações em linha"; e um outro ofício, desta feita da parte de Samuel Podberesky, Conselheiro-Geral Adjunto da secção de *Aviation Enforcement and Proceeding* do *Department of Transportation* (DOT), ao mesmo John Mogg, no sentido de explicar as funções desta entidade no âmbito da "protecção da privacidade dos consumidores relativamente às informações por estes facultadas às companhias de transportes aéreos".

À altura, e como vieram a revelar o escândalo *Wikileaks* espoletado por Julian Assange e as acções de Edward Snowden, antigo analista e administrador de sistemas da CIA e da NSA, já as agências de segurança dos EUA recolhiam e tratavam em "larga escala e de forma indiferenciada[25]"

---

[24] V. Disponível em: <https://build.export.gov/main/safeharbor/eu/eg_main_018475> (acedido a 23/07/2017).

[25] Para. 45 das Conclusões do Advogado-Geral Yves Bot, apresentadas em 23 de Setembro de 2015, no âmbito do Processo C-362/14 relativo ao pedido de decisão prejudicial apresentado pela *High Court* (Irlanda) ao Tribunal de Justiça no processo *Schrems*.

big data para efeitos de vigilância. Isto, tanto sobre cidadãos e entidades em território nacional como no estrangeiro, nomeadamente residentes ou com sede em território europeu, mesmo que não pudessem vir a interagir com os EUA.

Isto era conhecido da União, pelo menos, nas verificações periódicas que a Comissão levou a cabo, já que os EUA implementaram o programa PRISM por volta de 2007[26], tendo assim permitido que entidades como a NSA acedessem de forma quase livre a dados pessoais que estejam armazenados em servidores localizados nos territórios dos EUA[27]. Ou seja, a Comissão tinha conhecimento de que esta política poderia contrariar directamente quaisquer garantias estabelecidas nos princípios do "porto seguro" e de que ia para além de qualquer controlo que pudesse exercer *overseas*, mas preferiu manter a decisão de adequação[28].

---

[26] Greenwald, Glenn e Macaskill, Ewen. *NSA Prism program taps in to user data of Apple, Google and others*, the Guardian, de 7 de Junho de 2013. Disponível em: <https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data> (acedido a 28/06/2017).

[27] Para. 49 das Conclusões do Advogado-Geral Yves Bot no Processo C-362/14.

[28] A Comissão sabia deste programa, pelo menos, desde a avaliação periódica realizada em 2013, segundo a Comunicação 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 (COM(2013) 847 final, 27.11.2013). Não obstante ter conhecimento da gravidade da intromissão das entidades de segurança norte-americanas nos dados pessoais europeus e da desproporcionalidade, falta de transparência e utilização das informações para além do estritamente necessário em termos de segurança nacional, a Comissão decidiu manter o nível de adequação dos EUA. Aliás, curiosamente, somente o escândalo *Wikileaks* na base do caso *Schrems* teve a suficiente dimensão para pressionar as instituições europeias no sentido de alterarem a legislação e as práticas relativas aos níveis de adequação. Embora o acesso quase indiscriminado das agências aos dados recolhidos por empresas certificadas tivesse aparentemente levantado "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", a verdade é que as duas recomendações institucionais relativas ao acesso pelas autoridades dos EUA apenas vão num sentido 'informativo' de que "[a]s políticas de proteção da vida privada adotadas pelas empresas autocertificadas devem incluir informações sobre a medida em que a legislação dos EUA permite às autoridades públicas recolher e tratar dados transmitidos no âmbito do sistema de «porto seguro». Em especial, as empresas devem ser incentivadas a indicar, nas suas políticas de proteção da vida privada, se aplicam exceções ao sistema de «porto seguro» para observar requisitos de segurança nacional, interesse público ou execução legal" (recomendação 12); e que "[é] importante que a exceção por motivos de segurança nacional prevista na Decisão «porto seguro» seja utilizada apenas de forma

Donde, em primeiro lugar, o que quiçá importaria saber é se os membros da Comissão responsáveis pela 'investigação' das circunstâncias demonstrativas da adequação sabiam ou poderiam ter descoberto da (potencial) violação desse patamar mínimo por parte de algumas autoridades de vigilância e segurança, em virtude das suas atribuições e competências. E, em segundo lugar, se, assim sendo, deveriam ter incluído outro nível de compromissos nos acordos para acesso e processamento dos dados europeus.

Não é possível aferir se, no sentido de cumprir com o enunciado no n.º 2 do art. 25.º da Directiva 95/46/CE, foi sequer ponderada esta última hipótese, visto que a apreciação da adequação estava, de alguma forma, constrangida por dever ser levada a cabo em "função de todas as circunstâncias que rodeiem a transferência ou o conjunto de transferências de dados" (que seriam de foro estritamente comercial), e não imediatamente tendo em vista prospectivas 'rebuscadas' de utilização dos dados em investigações, de certo modo, secretas.

No entanto, segundo o mesmo enunciado, não só as regras gerais de Direito deveriam ser ponderadas como também as "medidas de segurança que são respeitadas" no país em questão, o que levanta dúvidas mais sobre a execução da lei pela Comissão e da ponderação de valores nas negociações do que propriamente sobre a suficiência do articulado de 1995. Por isso mesmo, aliás, não é de partilhar a opinião de doutrina como Olga Estadella-Yuste quando diz que a Directiva 95/46/CE não especifica se o *standard* de adequação se aplica à globalidade das leis de protecção da privacidade do país terceiro, a um sector, ou inclusivamente apenas às regras sobre o tipo de dados objecto das transferências propostas[29]. Parece ser claro que o nível de protecção só deveria ser definido com base no apuramento de todas as proposições normativas relevantes.

Um aspecto importante, relacionando as falhas no conceito e a concreta Decisão 2000/520/CE, é o que fica a descoberto relativamente ao balanço de competências entre os Estados-Membros e a Comissão quanto

---

proporcional e na medida em que for estritamente necessária" (recomendação 13) – algo que jamais seria, como a Comissão bem sabia, ou pelo menos deveria suspeitar.

[29] Estadella-Yuste, Olga. "Spain is on the road to implementing EU Directive 95/46", *International Review of Law, Computers & Technology*, vol. 11, issue 1, 1997, p. 40.

à fiscalização da adequação, no entendimento que parecia prevalecer ao nível institucional europeu antes do Acórdão *Schrems*[30].

Apesar de o n.º 3 do art. 25.º da Directiva 95/46/CE prever que os Estados-Membros e a Comissão se deveriam mutuamente informar quando considerassem que dado país terceiro não pareceria assegurar uma protecção adequada face ao manuseamento e tratamento dos dados pessoais, os números seguintes poderiam sugerir uma desconstrução de aparência da paridade. Segundo o n.º 4, somente a Comissão é que poderia "verificar" que dado país não asseguraria um nível de protecção adequado, na acepção feita no n.º 2[31]. Em consequência, os Estados-Membros deveriam proibir as transferências de dados daquela natureza para esse território e a Comissão, nos termos do n.º 5, deveria negociar com a jurisdição em causa para atender a este problema. Tal levaria a que ou o país fosse considerado como 'desadequado' a receber os dados pessoais dos cidadãos ou que a Comissão mantivesse a permissão para as transferências ao constatar que o país protegia a privacidade e as liberdades e direitos fundamentais de forma bastante, nos termos da sua "legislação interna ou dos seus compromissos internacionais".

Parece que o Comissário que respondeu a *Maximillian Schrems* aquando da sua queixa pela transferência de dados pessoais da *Facebook Ireland* para a *Facebook US*, interpretou o texto da Directiva 95/46/CE no sentido de que os Estados-Membros tinham, precisamente, um papel meramente informativo, quiçá mesmo acessório, na consideração do que seriam as medidas adequadas e suficientes a garantir a protecção dos dados pessoais fora das Comunidades. Aliás, à luz do desequilíbrio, o Comissário nem sequer terá interpretado o texto de forma exaustiva, visto que entendeu que uma investigação estaria imediatamente enviesada pelo facto de haver uma prévia decisão de adequação[32].

---

[30] Acórdão do TJ, C-362/14, ECLI:EU:C:2015:650, de 6 de Outubro de 2015.

[31] Na verdade, pelo facto de o n.º 2 não consignar uma definição do nível de protecção mas somente os critérios para aferir da sua existência, as remissões dos n.os 3, 4 e 6 e a linguagem, em geral, utilizada neste artigo, tornam-se algo difíceis de compreender.

[32] Para. 50 das conclusões do Advogado-Geral Yves Bot no Processo C-362/14. Levantam-se, porém, algumas dúvidas quanto ao entendimento do Comissário e, quiçá, de toda a Comissão quanto aos deveres necessários para manter a certeza e segurança jurídicas e o princípio do primado do Direito no ordenamento eurocomunitário perante esta resistência institucional

Apesar da capacidade técnica de algumas autoridades nacionais a este respeito, a decisão de adequação da Comissão, por mais contestada que fosse, marcaria o derradeiro entendimento sobre a adequação de protecção de dado país terceiro. Desta forma, o legislador europeu centralizaria a função, assegurando a necessária certeza jurídica. Mas, por outro lado, pareceria desnivelar de forma excessiva o contributo das APDs nacionais no âmbito da declaração e manutenção das decisões de adequação *vis-à-vis* os poderes da Comissão Europeia[33-34].

---

a investigar uma queixa, como se as decisões da Comissão não fossem, por exemplo, democraticamente passíveis de crítica.

[33] Aliás, no Acórdão do TJ, C-362/14, ECLI:EU:C:2015:650, para. 78, de 6 de Outubro de 2015, o Tribunal de Justiça da União Europeia sublinhou que, ponderando a relevância da protecção de dados pessoais no âmbito do direito fundamental ao respeito pela vida privada e o número potencialmente elevado de pessoas afectadas na sua intimidade caso o país terceiro não assegurasse uma adequada protecção, como acabou por suceder, a Comissão teria um poder de apreciação reduzido, muito possivelmente devido às suas competências e aos recursos de que dispõe, para averiguar estas situações. Assim sendo, o recurso às ADPs e a todas as ferramentas dos Estados aplicáveis é mais do que desejável – é verdadeiramente essencial no cumprimento da legislação europeia pela complexidade e volume das exigências decorrentes do art. 25.º da Directiva 95/46/CE, entre outras disposições, nomeadamente as do pacote legislativo de 2016.

[34] Também o Advogado-Geral Yves Bot obviou esta situação mas acabou por ler de forma diferente o texto do n.º 6 do art. 25.º da Directiva 95/46/CE, ao dizer que "é possível interpretar a Diretiva 95/46, e nomeadamente o seu artigo 25.º, n.º 6, bem como a Decisão 2000/520 num sentido que permita às autoridades nacionais conduzir as suas próprias investigações para estabelecer se a transferência de dados pessoais para um país terceiro satisfaz as exigências que decorrem dos artigos 7.º e 8.º da Carta", segundo o para. 46 das suas Conclusões ao Processo C-362/14. Igualmente no para. 86 virá reforçar o seu entendimento ao dizer que resultaria da economia do art. 25.º que a constatação em causa poderia ser levada a cabo quer pelos Estados-Membros quer pela Comissão. Assim sendo, numa importante análise *de iure*, tratar-se-ia de uma competência partilhada entre os Estados e as instituições. E, no para. 89, vai continuar, na mesma linha de pensamento, ao escrever que o artigo não acaba por atribuir à Comissão qualquer exclusividade em matéria de constatação do nível adequado quanto à proteção dos dados pessoais transferidos. Como antes, a economia do preceito demonstraria que os países também têm um papel relevante a desempenhar nesta matéria. Por fim, afere o Advogado-Geral que "uma decisão da Comissão desempenha, é certo, um papel importante na uniformização das condições de transferência válidas nos Estados-Membros. No entanto, essa uniformização só pode perdurar enquanto a constatação não for posta em causa", avançando, inclusivamente, com a ideia de que a avaliação da adequação poderá resultar de uma cooperação entre a Comissão e os Estados-Membros, no para. 91 das suas Conclusões.

Esta situação explica o entendimento do Tribunal de Justiça no caso *Schrems*[35]. Desde logo, o TJ avançou com a preocupação que subjaz a este trabalho, afirmando que:

> É certo que nem o artigo 25.º, n.º 2, nem nenhuma outra disposição da Diretiva 95/46 contêm uma definição do conceito de nível de proteção adequado. Em particular, o artigo 25.º, n.º 2, da referida diretiva limita-se a indicar que a adequação do nível de proteção oferecido por um país terceiro «será apreciada em função de todas as circunstâncias que rodeiem a transferência ou o conjunto de transferências de dados», e enumera, de modo não exaustivo, as circunstâncias que devem ser tomadas em conta ao proceder a tal apreciação[36].

O Tribunal também não avança com uma definição, mas continua a discorrer, nos trechos seguintes, sobre o nível de adequação. No para. 71 indica que, mesmo não havendo uma acepção *ex lata* do que seja o tal patamar, o n.º 6 do art. 25.º da Directiva impõe que os países terceiros o assegurem através da sua legislação, bem como dos compromissos internacionais de que sejam parte. Seguidamente, foca-se no elemento finalístico desta cláusula. A adequação deverá ser entendida e investigada tendo em vista o cumprimento da política expressa de protecção de dados pessoais à qual a União está obrigada, nos termos do n.º 1 do art. 8.º da CDFUE. E essa adequação deverá ser mantida pelo país terceiro, tal como se se aplicassem no seu território as disposições da Carta (para. 72)[37].

O termo 'adequado' indica, no entendimento do Tribunal, somente uma suficiência de protecção e não necessariamente um idêntico nível àquele garantido pela ordem jurídica da União. No entanto, igualmente na esteira do entendimento perfilhado pelo Advogado-Geral[38], isto deve

---

[35] Para um aprofundamento desta decisão, veja-se Lucas Pires, Martinho, "Algumas considerações sobre a compatibilidade do sistema de Privacy Shield com o direito da União Europeia à luz do acórdão Schrems", publicado neste Anuário.

[36] Acórdão do TJ, C-362/14, ECLI:EU:C:2015:650, para. 70, de 6 de Outubro de 2015.

[37] Também no para. 139 das Conclusões, Bot refere que o objectivo do artigo será o de "assegurar a continuidade da proteção conferida" em caso de transferência de dados pessoais para um país terceiro.

[38] No para. 141 das Conclusões, o Advogado-Geral refere que a avaliação do nível de adequação deverá ser feita nos termos do Direito e da prática do país em causa. Aquele será pronunciado dependendo da verificação de uma equivalência substancial de protecção à

significar que o país assegure efectivamente um resguardo "das liberdades e direitos fundamentais substancialmente equivalente ao conferido dentro da União (...). Com efeito, na falta de uma exigência desta natureza, o objetivo [de assegurar a continuidade do nível elevado dessa protecção em caso de transferência de dados pessoais para um país terceiro] seria ignorado[39]", tornando-se o processamento dos dados fora da União um modo de fugir à lei.

O Tribunal chegou ao ponto de deixar inclusivamente claro que a Comissão deveria verificar que a protecção dos dados pessoais é assegurada de forma holística e efectiva em todo o sistema jurídico do país terceiro considerado, independentemente de que meios utilize para o fazer na prática[40], algo que parece estar na base da mudança que o legislador europeu operou quanto a esta matéria em 2016. De facto, por detrás desta linguagem do TJ parece estar a crítica (e simultaneamente aviso para o futuro) de que havia a obrigação jurídica pendente sobre a Comissão de descobrir todas as alternativas possíveis à utilização dos dados pelas autoridades norte-americanas para lá do óbvio e imediato uso pelo DOC ou pelo DOT, fosse por que meios fosse, e de assegurar a substancial não ingerência nos dados para lá dos objectivos da Directiva, antes, durante e depois das negociações com os EUA.

Certamente que é preciso reconhecer que esta posição, em jeito *ex post*, é mais fácil e avisada do que à altura quiçá fosse previsível, no meio das negociações e muito antes da intrincada verdade verter para fora do controlo dos serviços secretos e de segurança dos EUA. Não obstante, a Comissão não é uma simples entidade qualquer, tem uma posição privilegiada que pode e deve usar no sentido de promover o interesse geral da União, *inter alia*, pelo controlo da aplicação do direito da União Europeia[41] (onde quer que ele deva ser aplicado, mesmo que externamente); e tem acesso, ou tem capacidade para ter acesso, a informações bem mais profundas e completas do que aquelas que pareceram satisfazê-la à altura – e até, mais tarde, nas periódicas análises da situação que lhe incumbem, a si e aos Estados, como

---

conferida pelas normas da União, independentemente dos meios pelos quais se processe e aplique a legislação estrangeira.

[39] Acórdão do TJ, C-362/14, ECLI:EU:C:2015:650, para. 73, de 6 de Outubro de 2015.

[40] Acórdão do TJ, C-362/14, ECLI:EU:C:2015:650, paras. 74 e 75, de 6 de Outubro de 2015.

[41] N.º 1 do art. 17.º do Tratado da União Europeia (TUE).

garantia do efeito útil nos termos dos n.os 1 a 3 do art. 25.º, conforme exige o n.º 6, da Directiva 95/46/CE, e como relembram o para. 76 deste Acórdão e os paras. 146 e 160 das Conclusões do Advogado-Geral[42].

Além disso, convém sublinhar paralelamente que o Tribunal de Justiça está, nestes parágrafos, a discutir a validade da Decisão 2000/520 e nunca a da Directiva 95/46/CE. São o direito e as práticas dos EUA que não asseguram um nível de protecção adequado na acepção do art. 25.º e não este trecho legal que é insuficiente, inválido ou que, na sua clareza e simplicidade, protege ineficazmente os direitos dos cidadãos europeus.

3. O Regulamento (UE) 2016/679

O RGPD[43] faz parte do mais recente pacote legislativo derivado da União Europeia relativamente à protecção de dados pessoais[44]. O texto vem afastar a Directiva 95/46/CE e propor um novo entendimento sobre o nível de protecção adequado que os países terceiros devem demonstrar para terem uma decisão de adequação por parte da Comissão. A inovação do n.º 1 do art. 45.º será no sentido de incluir as organizações internacionais a par com os países terceiros; além do esclarecimento de que, com uma decisão de adequação 'genérica', não serão necessárias autorizações específicas de cada vez que haja uma transferência de dados pessoais para esses destinatários.

---

[42] Uma obrigação contínua, *i.e.*, que se mantenha no tempo para lá da decisão inicial, de manutenção da adequação, segundo refere o Acórdão do TJ, C-362/14, ECLI:EU:C:2015:650, para. 147, de 6 de Outubro de 2015.

[43] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de Abril de 2016 relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Directiva 95/46/CE (RGPD).

[44] A ele juntam-se a Directiva (UE) 2016/680 do Parlamento Europeu e do Conselho de 27 de Abril de 2016 relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detecção ou repressão de infracções penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho, e a Proposta de Regulamento do Parlamento Europeu e do Conselho relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições, órgãos, organismos e agências da União e à livre circulação desses dados e que revoga o Regulamento (CE) n.º 45/2001 e a Decisão n.º 1247/2002/CE (9091/17 [2017/0002 (COD)], 24.05.2017).

Como dito, o legislador europeu não define o que entende por nível de protecção adequado e somente enuncia de forma não exaustiva os critérios que a Comissão deverá ter em conta na sua avaliação. Aqui, a inovação é substancial. Estamos, aliás, perante um caso excepcional de verborreia jurídica europeia cujos efeitos nas negociações da UE com os EUA em termos de capacidade de verificação dos compromissos deverão ser, na melhor das hipóteses, inexistentes. Nos termos do n.º 2 do art. 45.º do Regulamento, há agora que ponderar:

a) O primado do Estado de direito, o respeito pelos direitos humanos e liberdades fundamentais, a legislação pertinente em vigor, tanto a geral como a setorial, nomeadamente em matéria de segurança pública, defesa, segurança nacional e direito penal, e respeitante ao acesso das autoridades públicas a dados pessoais, bem como a aplicação dessa legislação e das regras de proteção de dados, das regras profissionais e das medidas de segurança, incluindo as regras para a transferência ulterior de dados pessoais para outro país terceiro ou organização internacional, que são cumpridas nesse país ou por essa organização internacional, e a jurisprudência, bem como os 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;
b) 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, responsáveis por assegurar e impor o cumprimento das regras de proteção de dados, e dotadas de poderes coercitivos adequados para assistir e aconselhar os titulares dos dados no exercício dos seus direitos, e cooperar com as autoridades de controlo dos Estados-Membros; e
c) Os compromissos internacionais assumidos pelo país terceiro ou pela organização internacional em causa, ou outras obrigações decorrentes de convenções ou instrumentos juridicamente vinculativos, bem como da sua participação em sistemas multilaterais ou regionais, em especial em relação à proteção de dados pessoais.

Como se pode verificar, este texto é bastante mais minucioso que o n.º 2 do art. 25.º da Directiva 95/46/CE. Não parece, porém, que este 'labor

legislativo' vá provocar um cuidado extra nas investigações periódicas encetadas pela Comissão ou uma sinceridade excepcional na definição das garantias de correcta utilização e protecção dos dados pessoais pelos países terceiros, muito menos os EUA.

4. O *Privacy Shield*

A Comissão não proferiu decisões típicas de adequação em 2000 nem em 2016 para as transferências de dados pessoais para os EUA, ambas à luz da Directiva 95/46/CE. Convém assim indagar porque é que este país terá o privilégio exclusivo de desenvolver, actualmente, um acordo para a transferência de dados que, não só já padece da singular falta de contrapartida, ou *trade-off*, que a UE imprimiu a esta legislação desde 1995 – visto que os países terceiros contratantes não têm de transferir os dados pessoais dos seus cidadãos para a União –, como mantém as regras de auto-certificação e se baseia no mesmo tipo de compromissos políticos e institucionais que permitiram a intromissão dos serviços de segurança nos dados pessoais dos cidadãos europeus. Se o sistema de "porto seguro" foi criticado por assentar em boa medida numa espécie de autoavaliação pelas empresas que participam voluntariamente neste sistema e por não ser acompanhado de garantias adequadas e de um mecanismo de fiscalização suficiente, o "escudo de protecção" poderá vir a ser alvo de semelhantes comentários por não se distinguir de forma significativa do acordo anterior, ao menos, neste aspecto[45].

Apesar de vir tentar responder às insuficiências do regime anterior, apontadas tanto pelo braço executivo como judiciário da União[46], não parece que seja o 'excesso linguísitco' adoptado pelo legislador europeu para o novo pacote de protecção de dados que vá garantir um efeito útil

---

[45] V. o seu funcionamento nos paras. introdutórios 30 e ss da Decisão de Execução (UE) 2016/1250 da Comissão de 12 de Julho de 2016 relativa ao nível de protecção assegurado pelo Escudo de Protecção da Privacidade UE-EUA, com fundamento na Directiva 95/46/CE do Parlamento Europeu e do Conselho (JO L 207, 1.8.2016).

[46] Lucas Pires, Martinho. "Algumas considerações sobre a compatibilidade do sistema de Privacy Shield com o direito da União Europeia à luz do acórdão Schrems", publicado neste Anuário.

de não ingerência nas informações pessoais dos cidadãos por agências de segurança de países terceiros, com os EUA à cabeça, ou que não surja, quiçá de forma bastante apropriada, um *Schrems II*[47].

A Comissão não modificou o seu *modus operandi* – ou, pelo menos, não anunciou nada a esse respeito – quanto à investigação que deveria legalmente fazer para assegurar que os interesses económicos e políticos não se sobrepõem à privacidade dos dados individuais, que, pelo menos por ora, ainda é um valor premente no quadro jurídico europeu, tanto primário como derivado.

A decisão de adequação da Comissão em relação aos EUA, à sombra da Directiva 95/46/CE, esclarecia sobre os compromissos e os textos norte-americanos sobre práticas comerciais e sobre as entidades que deverão tomar medidas contra práticas comerciais desleais e enganosas[48]. Mas não havia qualquer compromisso quanto à utilização dos dados fora do âmbito comercial, nomeadamente a proibição da sua utilização no seio de investigações criminais. Isto é, de certa forma, de estranhar pois que o nível de adequação só deve ser declarado se o país terceiro revelar todas as suas intenções relativamente ao uso dos dados, desde logo para efeitos de controlo e vigilância no combate ao terrorismo, criminalidade e situações afins.

Ora, a nova legislação europeia vem, e aí correctamente, elucidar os EUA (e talvez o próprio executivo europeu) que quando se fala em regras de direito gerais no presente contexto se quer dizer todas as regras que possam levar à utilização daqueles dados por uma qualquer entidade e para qualquer efeito, através de um exercício de 'exemplificação' e 'adjectivação' jurídicas. Como se lê na alínea a) do n.º 2 do art. 45.º acima citado, essas regras compreendem toda a "legislação *pertinente* em vigor, tanto a geral como a setorial, nomeadamente em matéria de segurança pública, defesa, segurança nacional e direito penal" (itálico adicionado). Assim sendo, consagrou o legislador europeu que os futuros compromissos com Estados

---

[47] Existindo já acções pendentes que poderão resultar nessa situação. V. Rücker, Daniel e Dienst, Sebastian, *Action for annulment against the EU-US Privacy Shield and coordinated review by German data protection authorities*, Noerr, de 10 de Novembro de 2016. Disponível em: <https://www.noerr.com/en/newsroom/News/action-for-annulment-against-the-eu-us-privacy-shield-and-coordinated-review-by-the-german-data-protection-authorities.aspx> (acedido a 16/10/2017).

[48] Anexo VII da Decisão 2000/520/CE.

terceiros não devem somente respeitar a abusos na utilização dos dados no âmbito de más práticas comerciais, mas também compreender todo o fenómeno de utilização desses dados, independentemente do seu fim.

É difícil que os autores da Directiva 95/46/CE previssem a utilização dos dados pessoais no âmbito da vigilância secreta pelos Estados. Não havia, aliás, uma atenção especial ao tratamento de dados por meios informáticos à altura. Mas, em bom rigor, não só a Directiva referia já, em 1995, as "regras de direito, gerais e sectoriais", como o fenómeno do uso de dados dos cidadãos no combate ao terrorismo e à criminalidade já estava consolidado. Será realmente necessário este desenvolvimento legislativo tão detalhado no art. 45.º do RGPD ou será sintomático de uma fraca capacidade de tratar do problema de forma eficaz, a nível executivo? E, mesmo existindo, será que vai surtir algum efeito, nomeadamente na conduta futura dos EUA?

Em defesa da União é possível dizer que não será uma tarefa fácil fazer com que países sem preocupações de protecção dos dados pessoais dos cidadãos como as presentes na legislação da União acabem por cumprir os diversos compromissos políticos e comerciais, *inter alia*, que originalmente estipulam nas conversações com os negociadores europeus. Vários factores explicam (embora não justifiquem) a dificuldade em manter o mesmo *standard* e a consequente utilização abusiva de dados alheios pelo controlo, real ou extrapolado, que isso permite às entidades de segurança e aos próprios governos. Basta pensar no clima de combate ao terrorismo a nível global através de meios intrusivos que incutem no público a ideia de que os governos estão, de facto, a fazer algo no sentido de dirimir ou diminuir a ameaça; na disponibilidade e quantidade de bases de dados comerciais com conteúdos e meta-informações variados e altamente detalhados; na prática estabelecida de vigilância interna sobre os próprios cidadãos da parte de certos Estados, que assim veem como necessários e naturalmente complementares o acesso e *profiling* dos dados de utilizadores externos de serviços, físicos ou electrónicos, nacionalmente localizados, entre outros.

A confiança política, económica e relativa a matérias de segurança do espaço europeu deveria ter saído, não obstante, seriamente fragilizada com a descoberta da utilização abusiva dos dados por parte dos EUA, tanto nas investigações de 2013 como no seguimento do fenómento *Wikileaks*. Donde, como agir em seguida? A Comissão decidiu esmiuçar até à exaustão somente os critérios de adequação e esperar que os novos compromissos de auto-certificação e as renovadas promessas tenham um efeito de externalidade

positiva sobre todas as instituições que podem processar ou imiscuir-se nos dados pessoais. Parece pouco salutar.

No acordo *privacy shield*[49], os compromissos norte-americanos acabam, desta vez, por passar igualmente pelo DOJ. Segundo o para. introdutório 125 da Decisão de Execução (UE) 2016/1250, o governo dos EUA terá apresentado determinadas garantias relativas a limitações e salvaguardas que, no sentido da avaliação da Comissão Europeia, devem demonstrar um nível de protecção adequado.

O documento não apresenta qualquer definição do que seja este patamar[50], à semelhança da legislação europeia, tanto nos parágrafos introdutórios

---

[49] Relembre-se que a Decisão de Execução (UE) 2016/1250 é ainda baseada no n.º 2 do art. 25.º da Directiva 95/46/CE e não no RGPD. É passível de discussão o conjunto de razões que terão levado a Comissão a não esperar pela entrada em vigor da nova legislação europeia em matéria de protecção de dados para basear o "escudo de protecção", especialmente quando algumas das preocupações do art. 45.º do Regulamento (UE) 2016/679 espelham, de uma forma quase inversa ao que seria normal de um ponto de vista da construção de um ordenamento jurídico, o que foi decidido entre a Comissão e as autoridades norte-americanas. No entanto, considerando que as apreciações periódicas ao acordo deverão ser feitas sobre este novo enquadramento e serão tanto o RGPD como a legislação conexa de 2016 a ditar os parâmetros para as futuras decisões sobre o nível de adequação dos países terceiros, assim se justifica a inclusão na secção anterior do novo trecho legal sobre transferências de dados pessoais de cidadãos da União Europeia para fora. Aliás, o G29 vem obviar igualmente esta situação ao dizer que, à luz do facto do *privacy shield* ter sido adoptado com base na Directiva de 1995, terá de ser consistente com o novo enquadramento europeu em termos de protecção de dados, tanto em finalidade como em escopo. O G29 sugeriu até, na Opinião 1/2016, adoptada a 13 de Abril de 2016 (16/EN, WP 238), 3, 15 e 58, que uma revisão seja encetada pouco depois da entrada em vigor do RGPD, no sentido de garantir que o elevado nível de protecção garantido nesse documento seja seguida pela decisão de adequação da Comissão. Algum tempo volvido, igualmente a AEPD veio reforçar esta linha de argumentação na sua Opinião 4/2016, adoptada a 30 de Maio de 2016, ao dizer que o art. 45.º do RGPD veio, de facto, criar novos requisitos para as transferências de dados baseadas numa decisão de adequação, como a Decisão de Execução (UE) 2016/1250.

[50] Infelizmente, o G29 não parece encontrar necessidade, nas suas conclusões relativas às clarificações recomendadas ao esboço da Decisão de Execução (UE) 2016/1250, nos termos da Opinião 01/2016, 57, de esclarecer o próprio conceito de nível de protecção adequado. Se o tivesse feito, talvez seria mais claro o conjunto de exigências da União nesta matéria de relações externas, visto que uma noção completa e legalmente bem construída seria mais adequada, clara e indicativa do que referências às circunstâncias em que decorrem as transferências de dados pessoais. Também na secção 4.3, designada "rumo a seguir", da Comunicação ao Parlamento Europeu e ao Conselho sobre a transferência transatlântica de dados: restaurar a

como no articulado. Não obstante, nos termos dos paras. introdutórios 126 e ss., é demonstrado como a Quarta Emenda à Constituição dos EUA[51] irá garantir a privacidade, dignidade e a protecção "contra atos arbitrários e invasivos por parte de funcionários do governo[52]". E muito embora as proposições constitucionais não recaiam sobre cidadãos estrangeiros, como as empresas que detêm os dados estão localizadas em território ou estão sob a alçada do direito norte-americano, aqueles beneficiarão de uma protecção indirecta[53].

Ademais, as "autoridades com funções coercivas [deverão] em qualquer caso obter autorização judicial (ou pelo menos respeitar o requisito de razoabilidade)", bem como respeitar as orientações do DOJ que limitem o acesso aos dados por motivos equivalentes aos critérios europeus de necessidade e proporcionalidade, como o uso dos "métodos de investigação menos invasivos possíveis", *vis-à-vis* o seu efeito sobre a privacidade e as demais liberdades cívicas dos titulares dos dados[54].

Ora, difícil é saber se este requisito de 'razoabilidade' irá suster a adequação da protecção perante a tenacidade das agências de segurança em obter grandes quantidades de informações pessoais, a qual é especialmente

---

confiança através de garantias sólidas (COM (2016) 117 final, 29.02.2016), a Comissão parece considerar que, embora se encarregue de encontrar e rever o nível adequado de protecção dos dados pessoais num ambiente dinâmico e vivo, por oposição ao paradigma estático que perpassava no "porto seguro", encontrar uma definição do que seja o nível de adequação não é uma componente essencial dessa adaptação às mudanças legislativas.

[51] Nos termos desta proposição constitucional, os cidadãos norte-americanos terão direito à inviolabilidade das suas pessoas, casas, documentos e outros bens pessoais contra buscas e apreensões não razoáveis. Ademais, ainda se consagra que não deverão ser emitidos mandatos a não ser sob causa provável, apoiada por juramento ou declaração, e com uma descrição específica do local sob investigação, bem como das pessoas ou coisas a serem apreendidas. V. a versão original com anotações e referências detalhadas. Disponível em: <http://uscode.house.gov/view.xhtml?path=/frontmatter/organiclaws/constitution&edition=prelim> (acedido a 29/6/2017).

[52] Para. introdutório 126 da Decisão de Execução (UE) 2016/1250.

[53] Muito embora, sejam de referir as dúvidas que o G29 avança nesta matéria. Diz o Grupo, na Opinião 01/2016, 55, que, mesmo que a protecção fosse efectiva, tal não significa que os meios de defesa dos interesses dos cidadãos estejam, de facto, ao alcance dos particulares, visto que o sujeito do direito a uma compensação efectiva neste cenário parece ser a companhia que recebe o pedido de acesso e não o(s) indivíduo(s) cujos dados estão em causa.

[54] Para. introdutório 127 da Decisão de Execução (UE) 2016/1250.

voraz se os dados ainda estiverem num estado quase cru, *i.e.*, pouco ou nada editados por intermediários. Nesta secção da Decisão, a Comissão demonstra até ter conhecimento de práticas norte-americanas que, não obstante a actualização do texto europeu, poderão continuar a perigar a protecção e secretismo dos dados pessoais[55]. Por outro lado, é interessante constatar que, apesar de "um certo número de vias de recurso judiciais para as pessoas singulares" (apresentados nos paras. introdutórios 130 a 132)[56], a Comissão conforta-se com factos como:

> [A]o abrigo da *Freedom of Information Act* (FOIA 5 U.S.C. § 552), qualquer pessoa tem o direito de obter acesso aos registos de uma agência federal e, após o esgotamento das soluções administrativas, de fazer valer esse direito em tribunal, exceto na medida em que esses registos sejam protegidos de divulgação pública por uma isenção ou uma exclusão especial decorrente do exercício de funções coercivas.

Somando à excepção referida no final deste parágrafo, é mister relembrar que as agências de segurança retiram as informações pessoais de forma,

---

[55] Disso são exemplo as excepcionais, mas existentes, buscas sem mandato. No para. introdutório 180 da Decisão de Execução (UE) 2016/1250, a Comissão enumera alguns dos casos de jurisprudência em que tal tenha sucedido, nomeadamente *Johnson c. Estados Unidos*, 333 U.S. 10, 14 (1948); *McDonald*, 335 U.S. 451, 453 (1948); *Camara c. Municipal Court*, 387 U.S. 523, 528 (1967); ou *G.M. Leasing Corp. c. Estados Unidos*, 429 U.S. 338, 352-53, 355 (1977). Por outro lado, o Supremo Tribunal de Justiça, alega a Comissão, tem periodicamente reforçado a ideia de que buscas realizadas fora de um processo judicial ou sem autorização prévia de um magistrado não tendem a ser razoáveis *per se*, na acepção constitucional. Mas, retomando, o para. introdutório 189 reforça as preocupações europeias ao dizer que, segundo as informações que a Comissão recebeu do governo norte-americano, há diversas situações que não necessitam de mandatos judiciais, como a actuação das autoridades no âmbito do *Electronic Communications Privacy Act* relativamente a "informações básicas sobre os assinantes, as sessões e a faturação (18 U.S.C. § 2703(c)(1), (2) (...) e [a] pedidos de acesso ao conteúdo de mensagens de correio eletrónico com mais de 180 dias (18 U.S.C. § 2703(b)", e as intimações administrativas, que estão fora desta exigência processual, muito embora sejam limitadas a casos concretos e, alegadamente, objecto de controlo jurisdicional independente, caso se executem em tribunal.

[56] V. as dificuldades relativas ao princípio da tutela jurisdicional efectiva em Lucas Pires, Martinho. "Algumas considerações sobre a compatibilidade do sistema de Privacy Shield com o direito da União Europeia à luz do acórdão Schrems", publicado neste Anuário.

obviamente, secreta e o acesso às suas bases de dados é, até agora, inédito, especialmente por cidadãos singulares, estrangeiros e fora do âmbito de um processo judicial. Assim sendo, torna-se difícil compreender quão adequada poderá realmente ser, na prática, esta garantia ao nível do patamar, nunca definido, de protecção de dados pessoais. Quiçá as reapreciações periódicas da verificação de adequação demonstrarão que o nível é suficiente, ou não[57]. Para já, os Estados Unidos comprometeram-se a informar a Comissão da evolução da legislação norte-americana, particularmente se se apresentar discordante do "escudo de protecção", tanto no domínio da protecção dos dados pessoais como no das limitações e garantias ao acesso das autoridades públicas a essas informações[58].

Numa nota positiva, convém referir que os anexos à Decisão de Execução (UE) 2016/1250 relativos aos compromissos dos EUA são bastante mais abrangentes, nomeadamente envolvendo mais entidades do sistema jurídico norte-americano na elaboração das garantias relativas à protecção dos dados pessoais e não se limitando aos princípios de aplicabilidade comercial, como sucedia previamente com a Decisão 2000/520/CE. Embora não avancem com quaisquer definições do nível de adequação e, de novo, fosse aconselhável que a Comissão tivesse levado a cabo um trabalho de campo, uma investigação de facto, que culminasse numa lista analisando toda a legislação interna e os compromissos internacionais dos EUA[59], os anexos consistem em: uma carta de Penny Pritzker, Secretária do Comércio, contendo um pacote de materiais que explicam tanto o funcionamento do *privacy shield* como o envolvimento e limitações das diversas autoridades[60]; um escrito

---

[57] Especialmente tendo sublinhado a Comissão de que as revisões não podem ser exercícios formais sem consequências e que as decisões de adequação não podem ser letra morta, na sua Comunicação (COM (2016) 117 final, 29.02.2016), 10. Numa curiosa formulação, a instituição disse ainda que as "*U.S. companies and authorities have to breathe life into the framework and continuously sustain it by living up to their commitments*" – infelizmente a tradução em Português está longe de correcta ou de carregar o mesmo impacto semântico ao dizer que "as empresas e as autoridades americanas têm de contribuir positivamente para o novo quadro e apoiar continuamente o seu funcionamento mediante o respeito dos seus compromissos".

[58] V. o para. introdutório 146 da Decisão de Execução (UE) 2016/1250.

[59] Eventualmente contando até com formas de acesso aos dados fora do âmbito estrito de vigilância e segurança nacionais, nos termos da Opinião 01/2016 do G29, 12.

[60] Neste pacote estão incluídos uma carta de Edith Ramirez, Presidente da FTC, que descreve a aplicação do "escudo de protecção", com um apêndice com uma descrição ampla

de Ken Hyatt, Subsecretário interino para as questões do comércio internacional, que, em representação da *International Trade Administration* (ITA), narra a melhoria da protecção dos dados pessoais que o quadro do *privacy shield* irá proporcionar, bem como os diversos compromissos que o DOC assumiu para a aplicação eficaz do acordo[61]; um desenvolvimento exaustivo dos princípios do quadro do "escudo de protecção de privacidade" (muito embora se assemelhe ao texto produzido anteriormente), baseado nas noções de adequação e razoabilidade; e uma carta de John Kerry, Secretário de Estado dos EUA à altura, felicitando o entendimento alcançado.

Por fim, a Comissão acabou por concluir que o ordenamento jurídico dos EUA consagra normas em vigor que limitam as ingerências, para efeitos coercivos ou outros de interesse público, aos direitos fundamentais dos cidadãos europeus cujos dados pessoais sejam transferidos da União ao abrigo do "escudo de protecção", no limite do necessário para a prossecução dos objectivos legítimos de investigação que levarem a cabo e dentro da protecção e certeza jurídicas legalmente exigidas[62]. Será a conclusão certa ou será antes a conclusão 'necessária' para os negócios europeus?

---

do sistema jurídico dos EUA em matéria de protecção da privacidade e da segurança; um ofício do DOT, assinado por Anthony Foxx, Secretário dos Transportes, semelhante ao texto anterior; duas missivas elaboradas pelo Conselheiro-Geral Robert Litt, do *Office of the Director of National Intelligence*, relativamente às garantias e limitações aplicáveis aos serviços de segurança nacional dos EUA na intromissão nos dados pessoais dos cidadãos europeus; uma outra carta e memorando em anexo do *Department of State*, informando do seu compromisso em instituir um novo Mediador para o Escudo de Protecção da Privacidade tendo em vista a apresentação de questões sobre as práticas norte-americanas de recolha de informação de origem eletromagnética; e um outro documento, desta feita subscrito por Bruce Swartz, Vice-Procurador-Geral Adjunto e Conselheiro para os Assuntos Internacionais, em representação do DOJ, sobre as garantias e limitações de acesso do governo dos EUA no exercício de funções coercivas e de interesse público pelos seus agentes e representantes públicos. Na missiva, a Secretária Pritzker sublinha ainda, com a seriedade possível, que a Comissária Věra Jourová, responsável da UE pela Justiça, Consumidores e Igualdade de Género "[p]ode ter a certeza de que os Estados Unidos da América encaram estes compromissos com seriedade".

[61] Entre os quais, merece destaque a resolução de cooperação com as APDs europeias na investigação e resolução de queixas.

[62] Paras. introdutórios 135 e ss. da Decisão de Execução (UE) 2016/1250.

Notas conclusivas

Os fluxos crescentes de dados pessoais a nível mundial impõem a adopção de medidas multilaterais que aproximem legislações, entidades, serviços e pessoas no sentido de se provocar um duplo, embora frágil, efeito. Por um lado, deve ser garantido um nível adequado de protecção para todos os titulares dos dados e, por outro, é mister acautelar para que não se levantem barreiras desnecessárias à livre circulação da informação, tanto pelos efeitos económicos[63] como pelas consequências sociais.

Não parece que a recente política legislativa europeia em matéria de transmissão de dados pessoais para países terceiros tenha, neste sentido, seguido a vereda mais eficaz. Especialmente em matérias complexas, propensas já de si a redundâncias e inutilidades técnico-linguísticas, a simplicidade da legislação é, das mais das vezes, a melhor escolha. Aliada a mecanismos *de iure*, mas também *de facto*, de verificação do cumprimento das normas, tanto melhor quanto mais descentralizados forem, a legislação não deve ser inutilmente prolixa na expectativa de que os destinatários e todos os demais afectados pelas normas percebam uma qualquer 'dica implícita de bom comportamento'.

É verdade que não é inteiramente seguro, ou sequer óbvio, que haja uma relação directa de efeito útil entre a consagração de um conceito de forma expressa e balizada e os problemas decorrentes de conseguintes decisões executivas (e administrativas) menos avisadas, baseadas na leitura e interpretação desse trecho legal que, não consagrando o conceito, se debruça sobre a sua essência. As decisões institucionais analisadas neste estudo basearam-se, segundo alguns autores, num conceito indeterminado ou flexível que, assim, melhor abrangeria as diferenças dos sistemas jurídicos dos países terceiros aquando das decisões de adequação. Mas a verdade é que esta 'insuficiência' legislativa tão gritante parece ter levado a alguma incerteza na elaboração dessas decisões e ter permitido a atitude subsequente dos EUA. Em suma, parece que esta 'abertura' do sistema não teve os efeitos que poderiam ter sido avistados originalmente.

O legislador europeu teve uma segunda oportunidade nesta matéria após o julgamento *Schrems*. Infelizmente, não teve a difícil, mas frutuosa,

---

[63] Cerda Silva, Alberto. "El «nivel adecuado de protección» para las transferencias internacionales de datos personales desde la Unión Europea", cit., p. 353.