COMISSÃO
EUROPEIA

Bruxelas, 27.11.2013
COM(2013) 847 final

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

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

(1) Introdução

A Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (a seguir designada «Diretiva relativa à proteção de dados») estabelece as regras aplicáveis às transferências de dados pessoais de Estados-Membros da UE para países terceiros [1] na medida em que essas transferências sejam abrangidas pelo âmbito desse instrumento[2].

Ao abrigo da Diretiva, a Comissão pode considerar que um país terceiro em causa assegura um nível de proteção adequado dos direitos das pessoas singulares por força do seu direito interno, ou de compromissos internacionais que assumiu, não se aplicando nesse caso as limitações específicas sobre as transferências de dados para esse país. Estas decisões são designadas habitualmente por «**decisões de adequação**».

Em 26 de julho 2000, a Comissão adotou a Decisão 520/2000/CE[3] (a seguir designada **Decisão «porto seguro»**) que reconhece que os princípios de «porto seguro» e as respetivas questões mais frequentes (FAQ) emitidos pelo Department of Commerce dos Estados Unidos da América, conferem um nível de proteção adequado às transferências de dados pessoais da União Europeia. A Decisão «porto seguro» foi tomada na sequência do parecer emitido pelo Grupo de Trabalho do Artigo 29.º e de um parecer do Comité do Artigo 31.º emitido por maioria qualificada dos Estados-Membros. Em conformidade com a Decisão 1999/468 do Conselho, a Decisão «porto seguro» foi submetida ao controlo prévio do Parlamento Europeu.

Por conseguinte, a atual Decisão «porto seguro» permite a transferência livre [4] de informações pessoais dos Estados-Membros da UE[5] para empresas estabelecidas nos EUA que tenham subscrito os princípios em circunstâncias em que, caso contrário, a transferência não respeitaria as normas da UE em termos da adequação do nível de proteção de dados, tendo em conta as diferenças consideráveis existentes entre os regimes dos dois lados do Atlântico.

O funcionamento do atual acordo de «porto seguro» baseia-se em compromissos, bem como na autocertificação das empresas participantes. Embora a assinatura destes acordos seja voluntária, as regras são vinculativas. Os seus princípios fundamentais são os seguintes:

---

1 Os artigos 25.º e 26.º da Diretiva relativa à proteção de dados definem o quadro jurídico aplicável às transferências de dados pessoais da UE para países terceiros não Partes do EEE.

2 A Decisão-Quadro 2008/977/JAI do Conselho, de 27 de novembro de 2008, relativa à proteção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal estabelece, no seu artigo 13.º, regras adicionais na medida em que essas transferências digam respeito a dados pessoais transmitidos ou disponibilizados por um Estado-Membro a outro Estado-Membro que posteriormente tencione transferir esses dados para um Estado terceiro ou organismo internacional para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou de execução de sanções penais.

3 Decisão 520/2000/CE da Comissão, de 26 de julho de 2000, 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, JO 215 de 28 de agosto de 2000, página 7.

4 O acima exposto não exclui a aplicação ao tratamento de dados de outros requisitos eventualmente previstos na legislação nacional que aplica a Diretiva relativa à proteção de dados.

5 As transferências de dados dos três Estados Partes no EEE são afetadas do mesmo modo, em conformidade com a extensão da Diretiva 95/46/CE ao Acordo do EEE, Decisão 38/1999 de 25 de junho de 1999, JO L 296 de 23.11.2000, página 41.

(a) Transparência das políticas de proteção da vida privada adotadas pelas empresas signatárias;

(b) Integração dos princípios de «porto seguro» nas políticas de proteção da vida privada das empresas;

(c) Aplicação coerciva, incluindo por parte das instâncias públicas.

Estes fundamentos essenciais do sistema «porto seguro» devem ser reexaminados para ter em conta **o novo contexto atual**, que se caracteriza pelos seguintes aspetos:

(a) Aumento exponencial dos fluxos de dados, anteriormente acessórios, mas atualmente essenciais para o rápido crescimento da economia digital, bem como os enormes progressos realizados em matéria de recolha, tratamento e utilização dos dados;

(b) Importância fundamental dos fluxos de dados, nomeadamente para a economia transatlântica,[6]

(c) O rápido crescimento do número de empresas estabelecidas nos EUA que subscrevem os princípios de «porto seguro» e que registou um aumento equivalente a oito vezes desde 2004 (tendo passado de 400 em 2004 para 3 246 em 2013);

(d) Informações publicadas recentemente sobre os programas de vigilância dos EUA, que levantam novas questões quanto ao nível da proteção que o acordo de «porto seguro» é suposto garantir.

Neste contexto, a presente Comunicação faz o ponto da situação sobre o funcionamento deste sistema. Baseia-se **em elementos** recolhidos pela Comissão, nos trabalhos do Grupo de Contacto UE/EUA sobre a proteção da vida privada realizados em 2009, num estudo levado a efeito em 2008 por um contratante independente [7], bem como em informações recebidas pelo Grupo de Trabalho UE/EUA (a seguir designado «Grupo de Trabalho»), criado na sequência das revelações constantes dos programas de vigilância americanos *(ver um documento paralelo).* A presente Comunicação inscreve-se na sequência dos dois **Relatórios de Avaliação da Comissão** realizados no período de arranque inicial do acordo «porto seguro», respetivamente em 2002[8] e 2004[9].

2. ESTRUTURA E FUNCIONAMENTO DO SISTEMA «PORTO SEGURO»

2.1. Estrutura do sistema «porto seguro»

Para subscrever os princípios de «porto seguro», uma empresa americana deve: a) estipular na sua política de proteção da vida privada, que deverá tornar pública, que subscreve os referidos princípios e que efetivamente os cumpre, e b) proceder à sua autocertificação, ou seja, declarar ao Department of Commerce dos EUA que cumpre os referidos princípios. A autocertificação deve ser renovada todos os anos. Os princípios de «porto seguro» relativos à

6 De acordo com alguns estudos, se os serviços e os fluxos transfronteiriços de dados forem perturbados devido à supressão das regras vinculativas para as empresas, das cláusulas contratuais-tipo e das regras de «porto seguro», o impacto negativo no PIB na UE poderá atingir entre 0,8 % e 1,3 % e as exportações de serviços da UE para os EUA poderão diminuir 6,7 % devido à perda de competitividade. Ver: «The Economic Importance of Getting Data Protection Right», estudo do Centro Europeu para Economia Política Internacional da Câmara de Comércio dos EUA, março de 2013.

7 Estudo de avaliação do impacto elaborado pela Comissão Europeia em 2008 pelo *Centre de Recherche Informatique et Droit* («CRID») da Universidade de Namur.

8 Documento de trabalho dos serviços da Comissão intitulado «Aplicação da Decisão 520/2000/CE da Comissão, de 26 de julho de 2000, nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho 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» SEC (2002) 196 de 13.12.2002.

9 Documento de trabalho dos serviços da Comissão «Aplicação da Decisão 520/2000/CE da Comissão 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», SEC (2004)1323 de 20.10.2004

proteção da vida privada, que figuram no anexo I da Decisão «porto seguro», incluem requisitos no que respeita à proteção dos dados pessoais (princípios de integridade dos dados, de segurança, de escolha e de retransferência), bem como os direitos dos titulares dos dados (princípios de aviso, de acesso e de aplicação efetiva).

No que respeita à execução do sistema «porto seguro» nos EUA, duas instituições americanas desempenham um papel preponderante: o Department of Commerce e a Comissão Federal do Comércio.

O **Department of Commerce** analisa todas as autocertificações efetuadas no âmbito do sistema de «porto seguro», bem como as respetivas renovações anuais que lhe são apresentadas pelas empresas, a fim de assegurar que contêm efetivamente todos os elementos necessários para participar no sistema[10]. O Department of Commerce atualiza a lista das empresas que apresentaram cartas de autocertificação, publicando-a, bem como as cartas, no seu sítio *Web*. Além disso, supervisiona o funcionamento do sistema «porto seguro» e suprime da lista as empresas que não cumprem os seus princípios.

No âmbito das suas competências em matéria de defesa do consumidor, a **Comissão Federal do Comércio** intervém contra práticas desleais e enganosas nos termos da Lei da Comissão do Comércio Livre, secção 5. As medidas de execução adotadas pela Comissão Federal do Comércio incluem inquéritos sobre declarações falsas relativas à adesão aos princípios de «porto seguro» e sobre a não-observância destes princípios por empresas que participam no sistema. O organismo competente nos casos específicos da aplicação dos princípios de «porto seguro» às transportadoras aéreas é o Department of Transportation dos EUA.[11]

A Decisão «porto seguro» faz parte integrante do direito comunitário de aplicação obrigatória pelas autoridades dos Estados-Membros. Nos termos desta Decisão, as **autoridades nacionais responsáveis pela proteção dos dados** dos Estados-Membros da UE têm o direito, em determinados casos, de suspender as transferências de dados para empresas certificadas «porto seguro»[12]. A Comissão não tem conhecimento de casos de suspensão por parte de uma autoridade nacional responsável pela proteção de dados ocorridos desde o estabelecimento dos princípios de «porto seguro», em 2000. Independentemente dos poderes de que gozam por força da Decisão «porto seguro», as autoridades nacionais da UE responsáveis pela proteção dos dados têm competência para intervir, nomeadamente no caso de transferências internacionais, a fim de garantir a observância dos princípios gerais que regem a proteção dos dados estabelecidos na Diretiva de 1995 relativa à proteção de dados.

Como o recorda a atual Decisão relativa ao «porto seguro», **compete à Comissão** – deliberando em conformidade com o procedimento de exame estabelecido no Regulamento 182/2011 – adaptar a Decisão, suspendê-la ou limitar o seu âmbito de aplicação a qualquer momento, à luz da experiência adquirida com a aplicação. Tal está previsto nomeadamente em caso de incumprimento sistemático da parte das autoridades americanas, por exemplo, se uma autoridade encarregada de garantir a observância dos princípios de «porto seguro» nos Estados Unidos não desempenhar efetivamente o seu papel ou se o nível de proteção proporcionado pelos princípios de «porto seguro» for ultrapassado por requisitos da legislação

---

10 Se a certificação ou recertificação da empresa não preencher os requisitos de «porto seguro», o Department of Commerce notifica a empresa solicitando-lhe que tome medidas (por exemplo, esclarecimentos, alterações na descrição da política da empresa), antes de a certificação poder ser finalizada.

11 Ver Código US, Título 49, Secção 41712.

12 Mais especificamente, a suspensão das transferências pode impor-se nas duas situações seguintes:
a) O organismo governamental nos EUA determinou que a empresa viola os princípios de «porto seguro».
b) Existam fortes probabilidades de os princípios de «porto seguro» estarem a ser violados; existam motivos razoáveis para crer que o mecanismo de execução não toma ou não irá tomar as decisões adequadas na altura devida para resolver o caso em apreço; a continuação da transferência dos dados pode criar um risco iminente de graves prejuízos para os titulares de dados em questão; e as autoridades competentes do Estado-Membro da UE realizaram, nesses casos, esforços razoáveis para informar a empresa e lhe dar a oportunidade de reagir:

norte-americana. Tal como sucede com qualquer outra decisão da Comissão, esta decisão também pode ser alterada por outras razões, ou mesmo revogada.

2.2. Funcionamento do sistema «porto seguro»

Entre as **3 246**[13] **empresas certificadas** figuram tanto pequenas como grandes empresas[14]. Embora os serviços financeiros e de telecomunicações não estejam sob a jurisdição da Comissão Federal do Comércio e estejam, por conseguinte, excluídos do sistema «porto seguro», entre as empresas certificadas figura um grande número de setores da indústria e dos serviços, incluindo empresas e indústrias da Internet muito conhecidas, que abrangem desde serviços informáticos e de informação a empresas farmacêuticas, serviços de viagens e turismo, serviços de saúde ou serviços de cartões de crédito.[15]. Trata-se essencialmente de empresas americanas que prestam serviços no mercado interno da UE. Existem também algumas filiais de empresas da UE, como a Nokia ou a Bayer. Destas empresas, 51 % processam dados de trabalhadores na Europa transferidos para os EUA para efeitos de gestão de recursos humanos[16].

Algumas das autoridades da UE responsáveis pela proteção de dados estão **cada vez mais preocupadas** pelas transferências de dados efetuadas no âmbito do atual sistema «porto seguro». Em alguns Estados-Membros, estas autoridades têm criticado o facto de os princípios serem formulados de forma muito geral, bem como de o quadro depender fortemente da autocertificação e da autorregulação. Várias empresas expressam preocupações da mesma ordem, apontando a existência de distorções de concorrência provocadas por uma aplicação insuficiente do sistema.

O atual acordo de «porto seguro» baseia-se na adesão voluntária de empresas aos respetivos princípios, na sua autocertificação e no controlo, por parte das autoridades públicas, do respeito dos compromissos assumidos aquando da autocertificação. Neste contexto, a falta de transparência e as eventuais deficiências a nível da aplicação podem comprometer os fundamentos em que assenta o sistema «porto seguro».

Com efeito, a falta de transparência ou insuficiências a nível da aplicação por parte dos EUA acarretam a transferência da responsabilidade para as autoridades europeias responsáveis pela proteção de dados, bem com para as empresas que utilizam o sistema. Em 29 de abril de 2010, as autoridades alemãs responsáveis pela proteção de dados adotaram uma decisão na qual solicitam às empresas que transferem dados da Europa para os Estados Unidos que verifiquem ativamente se as empresas americanas que importam dados respeitam efetivamente os princípios de «porto seguro» e recomendam que, «pelo menos, a empresa exportadora deve determinar se a certificação de «porto seguro» do importador continua válida»[17].

---

13 Em 26 de setembro de 2013 o número de organizações que participam no sistema de «porto seguro» consideradas «**current**» (atual) na Lista «porto seguro» era de **3 246,** e consideradas «**not current**» (não atual) **elevava-se a 935.**

14 Organizações que aderiram ao sistema de «porto seguro» com, no máximo, 250 empregados: 60**%** (1 925 de 3 246). Organizações que aderiram ao sistema de «porto seguro» com, pelo menos, 251 empregados: **40%** (1 295 de 3 246).

15 A título de exemplo, a MasterCard trabalha com milhares de bancos e constitui um bom exemplo de um caso em que o sistema «porto seguro» não pode ser substituído por outros instrumentos jurídicos para efeitos da transferência de dados pessoais, tais como normas vinculativas para as empresas ou disposições contratuais.

16 Organizações que aderiram ao sistema «porto seguro» e que tratam dados relativos aos recursos humanos em virtude da sua certificação «porto seguro» (e que, por conseguinte, aceitaram cooperar com as autoridades da UE responsáveis pela proteção dos dados, bem como conformar-se às suas regras): **51%** (1 671 de 3 246).

17 Ver Decisão Düsseldorfer Kreis de 28/29 de abril de 2010. Ver: Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich de 28./29 de abril de 2010 em Hanover: http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/290410_SafeHarbor.pdf?__blob=publicationFile No entanto, o titular da Autoridade Europeia para a Proteção de Dados (AEPD), Peter Hustinx, declarou, na audiência pública de 7 de outubro de 2013 consagrada a um inquérito da Comissão LIBE do Parlamento Europeu, que foram obtidas melhorias substanciais e que a maioria dos problemas relativos ao «porto seguro» está resolvida: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2013/13-10-07_Speech_LIBE_PH_EN.pdf

Em 24 de julho de 2013, na sequência das revelações sobre os programas de vigilância dos EUA, as autoridades alemãs responsáveis pela proteção de dados deram mais um passo, expressando a sua preocupação pelo facto de «ser altamente provável que os princípios consubstanciados nas decisões da Comissão não estejam a ser respeitados»[18]. Existem casos em que certas autoridades responsáveis pela proteção de dados (por exemplo, a autoridade de Bremen) solicitaram a uma empresa que transfere dados pessoais para fornecedores americanos que as informassem do modo como estes fornecedores impedem (se tal for o caso) a Agência Nacional de Segurança de aceder a esses dados. A autoridade irlandesa responsável pela proteção de dados indicou que recebera recentemente duas queixas relativamente ao programa «porto seguro», na sequência das revelações publicadas sobre os programas das Agências de Informações dos EUA, embora se tenha recusado a abrir um inquérito pelo facto de a transferência de dados pessoais para um país terceiro satisfazer os requisitos da legislação irlandesa em matéria de proteção de dados. Na sequência de uma queixa semelhante, a autoridade luxemburguesa responsável pela proteção de dados considerou que, aquando da transferência de dados para os EUA, as empresas Microsoft e Skype haviam respeitado a lei luxemburguesa relativa à proteção de dados [19]. No entanto, o Supremo Tribunal irlandês deferiu entretanto um pedido de recurso judicial, no âmbito do qual analisará a inação do Comissário irlandês para a proteção de dados relativamente aos programas de vigilância dos EUA. Uma destas duas queixas foi apresentada por um grupo de estudantes intitulado «Europe versus Facebook» (EVF), que submeteu igualmente uma queixa análoga contra a Yahoo na Alemanha, atualmente a ser examinada pelas autoridades competentes em matéria de proteção de dados.

Estas reações divergentes das autoridades responsáveis pela proteção de dados face a revelações sobre os programas de vigilância demonstram o risco real de fragmentação do sistema «porto seguro» e levantam questões quanto à sua implementação efetiva.

3. TRANSPARÊNCIA DAS POLÍTICAS DE PROTEÇÃO DA VIDA PRIVADA ADOTADAS PELAS EMPRESAS QUE PARTICIPAM NO SISTEMA

De acordo com a FAQ 6 que figura em anexo à Decisão «porto seguro» (anexo II), as empresas que pretendam certificar a sua adesão aos princípios de «porto seguro» devem comunicar a sua política em matéria de proteção da vida privada ao Department of Commerce e torná-la pública. Esta política deve incluir o compromisso de respeitar os princípios de proteção da vida privada. A obrigatoriedade de as empresas autocertificadas **tornarem públicas as suas políticas de proteção da vida privada** e de declararem a sua adesão aos princípios de proteção da vida privada constitui um elemento determinante para o funcionamento do sistema.

O facto de o acesso a estas políticas ser insuficiente prejudica as pessoas cujos dados pessoais são recolhidos e tratados, podendo constituir uma **violação do princípio de aviso**. Nesses casos, as pessoas cujos dados são transferidos a partir da UE podem não ter conhecimento dos seus direitos nem das obrigações a que está sujeita uma empresa objeto de autocertificação.

Além disso, o compromisso assumido pelas empresas de se conformarem aos princípios de proteção da vida privada **fundamenta o exercício das competências da Comissão Federal do Comércio para fazer aplicar estes princípios** em casos de incumprimento, adotando medidas contra empresas implicadas em práticas desleais ou enganosas. A falta de

18 Ver a resolução de uma conferência alemã dos comissários responsáveis pela proteção dos dados, que indica que os serviços de informações constituem uma enorme ameaça para a transmissão de dados entre a Alemanha e os países não-europeus. http://www.bfdi.bund.de/EN/Home/homepage_Kurzmeldungen/PMDSK_SafeHarbor.html?nn=408870

19 Ver o comunicado de imprensa, de 18 de novembro de 2013, da autoridade luxemburguesa responsável pela proteção de dados.

transparência das empresas nos Estados Unidos dificulta a vigilância exercida pela Comissão Federal do Comércio e compromete a eficácia da sua ação a nível da aplicação efetiva da lei.

Durante vários anos, um número considerável de empresas autocertificadas não publicou as suas políticas em matéria de proteção da vida privada, nem efetuou uma declaração pública de adesão aos princípios de proteção da vida privada. O relatório de 2004 relativo ao sistema «porto seguro» salientou a necessidade de o Department of Commerce **adotar uma posição mais ativa no que respeita ao controlo da observância** deste requisito.

Desde 2004, o Department of Commerce desenvolveu **novos mecanismos de informação** destinados a ajudar as empresas a cumprir as suas obrigações em matéria de transparência. As informações pertinentes sobre este sistema podem ser consultadas no sítio *Web* do Department of Commerce dedicado aos princípios de «porto seguro»[20], que permite igualmente às empresas carregar as suas políticas em matéria de proteção da vida privada. O Department of Commerce indicou que as empresas haviam recorrido a esta possibilidade e publicado as suas políticas em matéria de proteção da vida privada no seu sítio *Web* aquando do seu pedido de adesão ao sistema «porto seguro»[21]. Além disso, entre 2009 e 2013 o Department of Commerce publicou uma série de orientações para as empresas que tenham a intenção de aderir ao sistema «porto seguro», tais como o «Guide to Self-Certification» (guia da autocertificação) e «Helpful Hints on Self-Certifying Compliance» (conselhos úteis para uma autocertificação conforme).[22].

O grau de respeito das obrigações em matéria de transparência varia segundo as empresas. Se algumas delas se limitam a comunicar ao Department of Commerce uma descrição das suas políticas em matéria de proteção da vida privada no quadro do procedimento de autocertificação, a maioria publica essas políticas nos seus sítios *Web*, para além de efetuar o respetivo carregamento no sítio *Web* do Department of Commerce. No entanto, estas **políticas nem sempre são apresentadas de forma convivial e fácil de ler.** As ligações para as políticas em matéria de proteção da vida privada nem sempre funcionam de forma adequada nem reenviam sistematicamente para os sítios *Web* corretos.

Em conformidade com a Decisão e respetivos anexos, a obrigatoriedade de as empresas publicarem as suas políticas em matéria de proteção da vida privada **vai além da mera notificação** da auto-certificação ao Department of Commerce. Os requisitos a preencher para obter a certificação, enunciados nas FAQ, incluem a comunicação de uma descrição da política de proteção da vida privada e de informações transparentes sobre o sítio *Web* no qual o público pode consultar o texto dessas disposições[23]. As declarações relativas à política de proteção da vida privada devem ser claras e facilmente acessíveis ao público. Devem incluir uma ligação para o sítio *Web* do Department of Commerce consagrado ao «porto seguro», que contém uma lista dos membros atuais do sistema, bem como uma ligação para a entidade encarregada da resolução alternativa de conflitos. No entanto, uma série de empresas que aderiram ao sistema entre 2000 e 2013 não cumpriram estes requisitos. Aquando dos contactos realizados com a Comissão em fevereiro de 2013, o Department of Commerce reconheceu ser possível que até 10 % das empresas certificadas não publicaram nos seus sítios *Web* a sua política em matéria de proteção da vida privada, acompanhada de uma declaração de adesão aos princípios de «porto seguro».

---

20 http://www.export.gov/SafeHarbour/

21 https://SafeHarbour.export.gov/list.aspx

22 O Guia pode ser consultado no sítio *Web* do programa: http://export.gov/SafeHarbour/ Indicações úteis: http://export.gov/SafeHarbour/eu/eg_main_018495.asp

23 Em 12 de novembro de 2013, o Department of Commerce confirmou que: «Atualmente, as empresas que possuem um sítio *Web* público e que tratam dados relativos aos consumidores/clientes/visitantes devem incluir nos seus sítios *Web* uma descrição da sua política de proteção da vida privada conforme com os princípios de «porto seguro» (documento: «U.S.-EU Cooperation to Implement the Safe Harbor Framework» de 12 de novembro de 2013).

Estatísticas realizadas recentemente demonstram igualmente que continua a colocar-se o problema **da apresentação de declarações falsas de adesão ao sistema «porto seguro**. Cerca de 10 % das empresas que afirmam ter aderido ao sistema «porto seguro» não estão referenciadas pelo Department of Commerce como sendo membros atuais do sistema[24]. Estas declarações falsas proveem tanto de empresas que nunca participaram no sistema «porto seguro», como de empresas que, embora tenham participado no passado, posteriormente não voltaram a apresentar a sua autocertificação anual ao Department of Commerce. Nesse caso, essas empresas continuam a figurar no sítio *Web* consagrado ao sistema «porto seguro», mas o seu estatuto de certificação é «não atual», o que significa que por já terem sido membros do sistema têm a obrigação de continuar a assegurar a proteção de dados já tratados. A Comissão Federal do Comércio tem competência para intervir em casos de práticas fraudulentas e de incumprimento dos princípios de «porto seguro» (ver ponto 5.1). A falta de clareza quanto às «declarações falsas» compromete a credibilidade do sistema.

No decurso dos contactos que manteve regularmente com o Department of Commerce em 2012 e 2013, a Comissão Europeia alertou este último para o facto de que, para cumprirem as suas obrigações em matéria transparência, não basta que as empresas comuniquem ao Department of Commerce uma descrição da sua política em matéria de proteção da vida privada. Devem ainda colocar à disposição do público declarações sobre esta política. O Department of Commerce foi igualmente convidado a **intensificar os seus controlos periódicos dos sítios *Web* das empresas**, na sequência do procedimento de verificação aplicado no âmbito do primeiro procedimento de autocertificação ou da sua renovação anual, bem como a tomar medidas contra as empresas que não cumpram os requisitos em matéria de transparência.

Como primeira resposta às preocupações da UE, **o Department of Commerce tornou obrigatória, a partir de março de 2013,** a publicação no respetivo sítio *Web*, por parte das empresas que participam no sistema «porto seguro» e que possuem um sítio *Web*, da sua política de proteção da vida privada aplicável aos dados respeitantes aos clientes/utilizadores. Simultaneamente, o Department of Commerce começou a notificar todas as empresas cuja política em matéria de proteção da vida privada não comportava uma ligação para o sítio *Web* do Department of Commerce consagrado ao sistema «porto seguro» de que a deveriam introduzir, para que os consumidores que consultam os sítios *Web* dessas empresas tenham acesso direto à lista e ao sítio *Web* oficiais relativos ao sistema «porto seguro». Tal permitirá aos titulares de dados europeus verificar de forma imediata, sem buscas adicionais na Internet, os compromissos que uma determinada empresa comunicou ao Department of Commerce. Além disso, o Department of Commerce começou a informar as empresas de que nas suas políticas de proteção da vida privada publicadas na Internet deveria figurar o contacto da entidade independente encarregada da resolução de conflitos[25].

É necessário acelerar este processo para garantir que todas as empresas certificadas cumpram plenamente os requisitos do sistema «porto seguro» até março de 2014 (ou seja, até ao prazo previsto para a renovação da certificação anual das empresas, a contar da introdução de novos requisitos, em março de 2013).

---

24 Em setembro de 2013 o gabinete de consultoria australiano Galexia comparou as «declarações falsas» de adesão ao sistema «porto seguro» apresentadas em 2008 e em 2013. A sua principal constatação foi de que, paralelamente ao aumento do número de participantes neste sistema verificado entre 2008 e 2013 (de 1 109 para 3 246), o número de declarações falsas passou de 206 para 427. (http://www.galexia.com/public/about/news/about_news-id225.html).

25 Entre março e setembro de 2013, o Department of Commerce :
• Notificou as 101 empresas *que já tinham carregado a sua política de proteção da vida privada conforme com os princípios de «porto seguro» no sítio Web correspondente* de que deveriam igualmente fazer figurar essa política nos seus próprios sítios *Web*;
• Notificou as 154 empresas que ainda o não tinham feito de que deveriam incluir na sua política de proteção da vida privada uma ligação para o sítio *Web* consagrado ao «porto seguro»

Todavia, subsiste alguma preocupação quanto a saber se todas as empresas autocertificadas cumprem plenamente os requisitos em matéria de transparência. O Department of Commerce deverá proceder a controlos e inquéritos mais rigorosos para verificar o respeito das obrigações assumidas aquando da autocertificação inicial e da sua renovação anual.

4. INTEGRAÇÃO DOS PRINCÍPIOS DE «PORTO SEGURO» RELATIVOS À PROTEÇÃO DA VIDA PRIVADA NAS POLÍTICAS ADOTADAS PELAS EMPRESAS NESTA MATÉRIA

As empresas autocertificadas devem respeitar os princípios de proteção da vida privada definidos no anexo I da Decisão, de modo a obter e conservar as vantagens do sistema «porto seguro».

No relatório de 2004, a Comissão constatou que um grande número de **empresas não tinham incorporado corretamente os princípios de «porto seguro» relativos à proteção da vida privada** nas suas políticas de tratamento de dados. Por exemplo, as pessoas singulares nem sempre recebiam informações claras e transparentes sobre a finalidade do tratamento dos seus dados ou não lhes era dada a possibilidade de recusar que os seus dados fossem comunicados a terceiros ou utilizados para fins incompatíveis com os fins para os quais haviam sido inicialmente coligidos. No seu relatório de 2004, a Comissão considerava que o Department of Commerce dos EUA *deveria ser mais ativo no que respeita ao acesso ao sistema «porto seguro», bem como à sensibilização para os seus princípios*[26].

Os progressos registados a este respeito são limitados. Desde 1 de janeiro de 2009, a política de proteção da vida privada de uma empresa que pretenda renovar o seu estatuto de certificação «porto seguro» — que deve ser renovado todos os anos — será avaliada previamente pelo Department of Commerce antes da renovação. No entanto, esta avaliação tem um âmbito limitado. **Não é realizada uma avaliação completa das práticas efetivas** nas empresas autocertificadas, o que reforçaria de forma significativa a credibilidade do procedimento de autocertificação.

Na sequência dos apelos da Comissão para uma supervisão mais rigorosa e sistemática das empresas autocertificadas por parte do Department of Commerce, **este último presta atualmente uma maior atenção às novas certificações**. Entre 2010 e 2013, aumentou substancialmente o número de novas certificações que não foram aceites e que foram devolvidas às empresas para que introduzissem melhorias nas suas políticas de proteção da vida privada[27]. O Department of Commerce assegurou à Comissão que só poderão ser efetuadas certificações ou renovações de certificações se a política de proteção da vida privada das empresas preencher todos os requisitos, devendo incluir nomeadamente um compromisso afirmativo de adesão ao conjunto de princípios de «porto seguro» pertinentes relativos à proteção da vida privada, e se essa política estiver acessível ao público. As empresas devem obrigatoriamente identificar, no seu registo da lista de participantes do sistema «porto seguro», o sítio *Web* no qual está publicada a sua política nesta matéria. Devem também indicar claramente no seu sítio *Web* o nome de uma entidade encarregada da resolução alternativa de conflitos e incluir uma ligação para a autocertificação em matéria dos princípios de «porto seguro» no sítio *Web* do Department of Commerce. No entanto, estima-

[26] Ver página 8 do Relatório de 2004, SEC(2004) 1323.

[27] Segundo as estatísticas publicadas em setembro de 2013, o Department of Commerce contactou em 2010 18 % (93) das 512 empresas que receberam a sua primeira certificação e 16 % (231) das 1 417 empresas que a renovaram, exortando-as a introduzir melhoramentos nas suas políticas de proteção da vida privada e/ou nos seus pedidos de adesão ao sistema «porto seguro». No entanto, em resposta aos pedidos da Comissão no sentido de que todos os pedidos sejam objeto de controlos rigorosos, diligentes e sistemáticos, o Department of Commerce contactou, a partir de meados de setembro, 56 % (340) das empresas que receberam a sua primeira certificação e 27 % (493) das empresas que a renovaram, solicitando-lhes que introduzissem melhoramentos nas suas políticas de proteção da vida privada.

se que 30 % dos participantes no sistema «porto seguro» não incluem, nos seus sítios *Web* [28], informações relativas à resolução de conflitos no contexto das suas políticas de proteção da vida privada.

A maioria das empresas que o Department of Commerce retirou da lista do sistema «porto seguro» foram suprimidas a pedido explícito das próprias (por exemplo, empresas que haviam sido objeto de fusões ou de aquisições, que tinham mudado de ramo de atividade ou que tinham cessado a atividade). Foi suprimido da lista um número mais pequeno de empresas que encerraram a sua atividade quando se verificou que os seus sítios *Web* mencionados na lista aparentemente já não estavam operacionais e que a sua certificação era «não atual» desde há vários anos [29]. Importa observar que nenhuma destas supressões se ficou a dever ao facto de o Department of Commerce ter detetado problemas de conformidade.

O registo na lista dos participantes do sistema «porto seguro» funciona como um anúncio público e como um registo dos compromissos assumidos pelas empresas que nela figuram. **O compromisso de aderir aos princípios de «porto seguro» não é limitado no tempo** no que respeita aos dados recebidos durante o período em que a empresa beneficia das vantagens do sistema «porto seguro», devendo esta continuar a aplicar estes princípios durante todo o período em que armazena, utiliza ou comunica esses dados, mesmo se deixar de participar no sistema por qualquer motivo.

As empresas que pediram para aderir ao sistema «porto seguro» **mas cujo pedido foi rejeitado no controlo administrativo** realizado pelo Department of Commerce e que, por esse motivo, nunca foram inscritas na lista de participantes repartem-se do seguinte modo: **em 2010**, só **6%** (33) das 513 empresas que receberam a sua primeira certificação nunca tinham sido inscritas nesta lista por não cumprirem as normas que regem a autocertificação estabelecidas pelo Department of Commerce. Em **2013, 12 %** (75) das 605 empresas que receberam a sua primeira certificação nunca tinham sido inscritas nesta lista por não cumprirem as normas que regem a autocertificação estabelecidas pelo Department of Commerce.

Para aumentar a transparência dos seus controlos, o Department of Commerce deverá, pelo menos, indicar no seu sítio *Web* todas as empresas que tenham sido excluídas do sistema «porto seguro», mencionando os motivos que o levaram a não renovar a sua certificação. É conveniente que se deixe de considerar como mera informação o estatuto de «não atual» que figura na lista dos participantes no sistema «porto seguro» do Department of Commerce: esta menção deverá ser acompanhada de **uma advertência clara**, tanto escrita como gráfica, que indique que atualmente a empresa em questão não preenche os requisitos do sistema «porto seguro».

Além disso, algumas empresas ainda não integraram completamente todos os princípios de «porto seguro» nas suas políticas. Para além da questão da transparência, abordada no ponto 3, as políticas de proteção da vida privada adotadas pelas empresas autocertificadas são muitas vezes pouco claras quanto aos fins a que se destina a recolha de dados, bem como ao direito de decidir se os dados podem ou não ser divulgadas a terceiros; o respeito dos princípios de «aviso» e de «escolha» suscita, pois, alguma preocupação. O aviso e a escolha são elementos determinantes para garantir que os titulares dos dados tenham um controlo sobre o tratamento que é dado aos seus dados pessoais.

---

28 Intervenção de Chris Connolly (Galexia) perante a Comissão LIBE do Parlamento Europeu, em 7 de outubro de 2013.

29 Em dezembro de 2011, o Department of Commerce dos EUA havia retirado 323 empresas da lista de participantes no sistema «porto seguro»: 94 empresas foram retiradas por cessação de atividade, 88 por terem sido objeto de fusões ou de aquisições, 95 a pedido da empresa-mãe, 41 por não terem solicitado, por várias vezes, a recondução da certificação, e 5 por razões várias.

Atualmente, não está suficientemente garantida a primeira etapa decisiva do processo de cumprimento, a saber, a integração dos princípios de «porto seguro» nas políticas das empresas relativas à proteção da vida privada. O Department of Commerce deverá abordar prioritariamente esta questão, desenvolvendo uma metodologia de cumprimento destinada às empresas, tanto em termos das suas práticas de funcionamento, como da sua interação com os clientes. Em vez de aplicar medidas de controlo unicamente com base em queixas apresentadas por pessoas singulares, **o Department of Commerce deverá acompanhar de perto a integração efetiva dos princípios de «porto seguro» nas políticas das empresas em matéria de proteção da vida privada**.

5. APLICAÇÃO POR PARTE DAS INSTÂNCIAS PÚBLICAS

Existem vários mecanismos para assegurar a aplicação eficaz do sistema «porto seguro» e oferecer a possibilidade de recurso às pessoas cuja proteção dos seus dados pessoais seja afetada pelo incumprimento dos princípios que regem a proteção da vida privada.

Em conformidade com o princípio de «aplicação», as políticas em matéria de proteção da vida privada adotadas pelas organizações autocertificadas devem comportar mecanismos de cumprimento eficazes. Em conformidade com o princípio de «aplicação», como explicitado nas FAQ 11, 5 e 6, esta obrigação pode ser preenchida pela adesão a **mecanismos de recurso independentes** que tenham declarado publicamente a sua competência para tratar queixas apresentadas por pessoas singulares relativas ao não cumprimento dos princípios do sistema «porto seguro». A título alternativo, a empresa pode comprometer-se a cooperar com o **Painel de Proteção de Dados da UE**[30]**.** Além disso, as empresas autocertificadas estão sob a jurisdição da Comissão Federal do Comércio nos termos do ponto 5 do *Federal Trade Commission Act*, que proíbe práticas ou atos desleais ou fraudulentos no domínio do comércio[31].

O relatório de 2004 dava conta de alguma preocupação no que diz respeito à aplicação do sistema «porto seguro», indicando nomeadamente que a Comissão Federal do Comércio deverá ser mais ativa em termos da abertura de inquéritos e da sensibilização das pessoas singulares para os seus direitos. Outra questão objeto de alguma preocupação era a falta de clareza no que se refere à competência desta Comissão para controlar a aplicação dos princípios de «porto seguro» relativos a dados sobre recursos humanos.

O organismo de recurso competente em matéria de dados sobre recursos humanos — Painel de Proteção dos Dados da UE — recebeu uma queixa relativa a esse tipo de dados [32]. Todavia, a quase inexistência de queixas não permite tirar conclusões quanto ao correto funcionamento do sistema. Seria conveniente instaurar controlos sistemáticos para verificar a aplicação efetiva dos compromissos assumidos pelas empresas participantes em matéria de proteção de dados. As autoridades responsáveis pela proteção dos dados na UE devem igualmente tomar medidas para sensibilizar os cidadãos para a existência do Painel.

---

30 O Painel de Proteção de Dados da UE tem competência para instruir e resolver queixas apresentadas por pessoas singulares por alegado incumprimento dos princípios de «porto seguro» por parte de empresas americanas membros deste sistema. As empresas que certificam que respeitam os princípios de «porto seguro» devem optar por aderir a um mecanismo de recurso independente ou por cooperar com o Painel de Proteção de Dados da UE para solucionar problemas decorrentes do incumprimento dos princípios de «porto seguro». No entanto, a cooperação com o Painel de Proteção de Dados da UE é obrigatória nos casos em que a empresa americana em questão trata dados pessoais respeitantes a recursos humanos transferidos da União no âmbito de uma relação de trabalho. Se a empresa se comprometer a cooperar com o Painel de Proteção de Dados da UE, deve comprometer-se igualmente a respeitar todas as recomendações formuladas pelo mesmo caso este considere que a empresa deve tomar medidas específicas para cumprir os princípios de «porto seguro», incluindo medidas corretivas ou compensatórias.

31 O Department of Transportation exerce competências análogas relativamente às transportadoras aéreas ao abrigo do Código dos Estados Unidos, Título 49, secção 41712.

32 A queixa foi apresentada por um cidadão suíço e, por conseguinte, foi submetida pelo Painel de Proteção dos Dados da UE à autoridade nacional de proteção de dados suíça (os EUA têm um sistema «porto seguro» separado para a Suíça).

Foram salientados alguns problemas a nível do funcionamento das instâncias e organismos de resolução alternativa de litígios na sua qualidade de órgãos de aplicação efetiva. Alguns destes organismos não dispõem de meios suficientes para resolver os casos de não respeito dos princípios de «porto seguro», pelo que é necessário colmatar esta lacuna.

5.1. Comissão Federal do Comércio

A Comissão Federal do Comércio pode tomar medidas coercivas em caso de violação, por parte das empresas, dos compromissos que assumiram relativamente aos princípios de «porto seguro». Quando o sistema «porto seguro» foi criado, a Comissão Federal do Comércio comprometeu-se a examinar prioritariamente todos os *dossiers* que lhe haviam sido submetidos pelas autoridades dos Estados-Membros da UE[33]. Como durante os primeiros dez anos do acordo de «porto seguro» não recebeu quaisquer queixas, a Comissão Federal do Comércio decidiu procurar detetar eventuais violações aos princípios de «porto seguro» em cada inquérito que realizava em matéria da vida privada e da segurança dos dados. Desde 2009, esta Comissão instaurou 10 processos coercitivos contra empresas por violação dos princípios de «porto seguro». Estes processos traduziram-se, nomeadamente, em injunções — sob reserva de pesadas multas — que proíbem as declarações falsas em matéria de proteção da vida privada, incluindo no que se refere ao respeito dos princípios de «porto seguro», e que impõem às empresas programas exaustivos de proteção da vida privada, bem como auditorias durante 20 anos. A pedido da Comissão Federal do Comércio, as empresas em questão devem submeter o seu programa de proteção da vida privada a avaliações independentes, que serão comunicadas regularmente a esta última. As injunções da Comissão Federal do Comércio proíbem igualmente estas empresas de efetuarem declarações falsas quanto às suas práticas em matéria de proteção da vida privada, bem como à sua participação no sistema «porto seguro» ou em sistemas semelhantes de proteção da vida privada. Foi o que decidiu, por exemplo, a Comissão Federal do Comércio na sequência dos inquéritos que realizou às empresas Google, Facebook e Myspace.[34] Em 2012, a Google aceitou pagar uma multa de 22,5 milhões de dólares US para pôr termo a alegações segundo as quais teria infringido uma injunção («*consent order*»). Em todos os inquéritos relativos a violações da vida privada, a Comissão Federal do Comércio examina sistematicamente se existe uma violação do sistema «porto seguro».

A Comissão Federal do Comércio reiterou recentemente as suas declarações e o seu compromisso de examinar, a título prioritário, os *dossiês* recebidos das empresas autoregulamentadas em matéria de proteção da vida privada e dos Estados-Membros da UE sobre alegações de incumprimento dos princípios de «porto seguro».[35] Nos últimos três anos, a Comissão Federal do Comércio recebeu apenas um número reduzido de *dossiês* provenientes das autoridades europeias responsáveis pela proteção de dados.

A cooperação transatlântica entre as autoridades de proteção de dados começou a desenvolver-se nos últimos meses. Assim, em 26 de junho de 2013, a Comissão Federal do

---

33 Ver anexo V da Decisão 2000/520/CE da Comissão, de 26 de julho de 2000.

34 Entre 2009 e 2012, a Comissão Federal do Comércio concluiu 10 processos coercitivos relativos a casos de violações de compromissos a título do sistema «porto seguro»: FTC v. Javian Karnani, and Balls of Kryptonite, LLC (2009), World Innovators, Inc. (2009), Expat Edge Partners, LLC (2009), Onyx Graphics, Inc. (2009), Directors Desk LLC (2009), Progressive Gaitways LLC (2009), Collectify LLC (2009), Google Inc. (2011), Facebook, Inc. (2011), Myspace LLC (2012). Ver: "Federal Trade Commission of Safe Harbour Commitments": http://export.gov/build/groups/public/@eg_main/@SafeHarbour/documents/webcontent/eg_main_052211.pdf Ver igualmente: "Case Highlights": http://business.ftc.gov/us-eu-Safe-Harbour-framework. A maior parte destes litígios diziam respeito a empresas que tinham aderido ao sistema «porto seguro», mas que posteriormente continuaram a declarar que eram participantes, embora não tivessem renovado a sua certificação anual.

35 Julie Brill, Membro da Comissão Federal do Comércio, reiterou este compromisso numa reunião realizada com as autoridades europeias responsáveis pela proteção de dados (Grupo criado nos termos do Artigo 29.º) em Bruxelas, em 17 de abril de 2013.

Comércio assinou com a autoridade irlandesa de proteção de dados um memorando de entendimento sobre assistência mútua em matéria de aplicação da legislação que protege os dados pessoais no setor privado. Este memorando de entendimento estabelece um quadro para intensificar, racionalizar e tornar mais eficaz a cooperação em matéria de controlo do respeito da proteção da vida privada[36].

Em agosto de 2013, a Comissão Federal do Comércio anunciou um novo reforço das fiscalizações às empresas que controlam grandes bases de dados pessoais. Criou igualmente um portal no qual os consumidores podem apresentar queixa contra uma empresa americana por violação da vida privada [37].

A Comissão Federal do Comércio deverá igualmente redobrar de esforços para investigar as falsas alegações de adesão ao sistema «porto seguro». Uma empresa que afirma no seu sítio *Web* que cumpre os requisitos do sistema «porto seguro», mas que não figura na lista do Department of Commerce na qualidade de membro «atual» induz em erro os consumidores e abusa da sua confiança. As declarações falsas enfraquecem a credibilidade geral do sistema, pelo que devem ser imediatamente retiradas dos sítios *Web* das empresas. Estas devem ficar vinculadas pela condição obrigatória de não induzir em erro os consumidores. A Comissão Federal do Comércio deve continuar a procurar detetar declarações falsas de adesão ao sistema «porto seguro», como no caso *Karnani*, no qual decretou o encerramento de um sítio *Web* criado e explorado por empresas estabelecidas na Califórnia que se reclamavam, abusivamente, participantes no sistema e se dedicavam a práticas fraudulentas de comércio eletrónico de que eram vítimas consumidores europeus[38].

Em 29 de outubro de 2013, a Comissão Federal do Comércio anunciou que, nos meses anteriores, tinha dado início a um grande número de investigações relativas ao respeito dos princípios de «porto seguro» e que era provável que iniciasse mais ações nesta matéria nos próximos meses. Confirmou igualmente que estava decidida a procurar formas de melhorar a sua eficácia e que continuaria a acolher favoravelmente qualquer pista concreta, como a queixa recebida no mês anterior de um defensor dos direitos dos consumidores estabelecido na Europa que dava conta de um grande número de violações dos princípios de «porto seguro».[39] A Agência comprometeu-se ainda a controlar «de forma sistemática o cumprimento das injunções relativas ao sistema «porto seguro», como aliás de todas as injunções»[40].

Em 12 de novembro de 2013, a Comissão Federal do Comércio informou a Comissão Europeia de que **«se a política de proteção da vida privada de uma empresa promete proteções conformes com o sistema «porto seguro», a omissão por esta empresa de se registar ou de renovar o seu registo não escusa, por si só, a empresa de se submeter à aplicação coerciva, pela Comissão Federal do Comércio, dos seus compromissos em matéria de «porto seguro»**[41].

Em novembro de 2013, o Department of Commerce informou a Comissão Europeia de que para «garantir que as empresas não apresentem «declarações falsas» de adesão ao sistema «porto seguro», começará a contactar os participantes no sistema, um mês antes da data de

---

36 http://www.dataprotection.ie/viewdoc.asp?Docid=1317&Catid=66&StartDate=1+January+2013&m=n

37 Os consumidores americanos podem apresentar as suas queixas no portal criado para o efeito pela Comissão Federal do Comércio (https://www.ftccomplaintassistant.gov/) e os consumidores estrangeiros podem apresentar queixa no sítio *Web* http://www.econsumer.gov.

38 http://www.ftc.gov/os/caselist/0923081/090806karnanicmpt.pdf

39 http://www.ftc.gov/speeches/brill/131029europeaninstituteremarks.pdf e http://www.ftc.gov/speeches/ramirez/131029tacdremarks.pdf

40 Carta da Presidente da Comissão Federal do Comércio, Edith Ramirez, à Vice-Presidente da Comissão Viviane Reding.

41 Carta da Presidente da Comissão Federal do Comércio, Edith Ramirez, à Vice-Presidente Viviane Reding.

renovação da sua certificação, para lhes indicar as etapas a seguir caso decidam não proceder a essa renovação». **O Department of Commerce irá intimar as empresas** nesta categoria a retirarem todas as referências à sua participação no sistema «porto seguro», incluindo a utilização da marca de certificação correspondente, das suas políticas de proteção da vida privada e dos seus sítios *Web*, **e notificá-las de forma clara que caso não o façam poderão ficar sujeitas a processos coercitivos por parte da Comissão Federal do Comércio**»[42].

Para lutar contra o fenómeno das declarações falsas de adesão ao sistema «porto seguro», as políticas de proteção da vida privada publicadas pelas empresas autocertificadas nos seus sítios *Web* devem incluir sistematicamente uma ligação para o sítio *Web* do Department of Commerce consagrado ao sistema «porto seguro», no qual são enumerados todos os membros «atuais» do sistema. Os titulares de dados europeus poderão assim verificar de forma imediata, sem buscas adicionais, se uma determinada empresa é um membro atual do sistema. Em março de 2013, o Department of Commerce começou a impor esta exigência às empresas, mas este processo deverá ser intensificado.

A monitorização permanente pela Comissão Federal do Comércio e o consequente controlo da aplicação efetiva dos princípios do «porto seguro» — para além das medidas adotadas pelo Department of Commerce assinaladas acima — continuam a ser uma prioridade essencial para assegurar o funcionamento correto e eficaz do sistema. É necessário, nomeadamente, aumentar o número de **verificações e inquéritos sistemáticos para garantir o respeito, por parte das empresas,** dos princípios de «porto seguro». A apresentação de queixas relativas a violações junto da Comissão Federal do Comércio deverá igualmente ser facilitada.

5.2. Painel de proteção dos dados da UE

O Painel de proteção dos dados da UE é um órgão criado ao abrigo da Decisão «porto seguro». Tem competência para investigar queixas apresentadas por particulares relativamente a dados pessoais recolhidos no âmbito de relações de trabalho, bem como os casos de empresas certificadas que optaram por esta solução para a resolução de litígios no âmbito do sistema «porto seguro» (53 % das empresas). É composto por representantes das diferentes autoridades de proteção dos dados da UE.

Até à data, o Painel recebeu quatro queixas (duas em 2010 e duas em 2013). Em 2010, o Painel remeteu duas queixas para as autoridades nacionais de proteção de dados (Reino Unido e Suíça). A terceira e quarta queixas estão atualmente a ser examinadas. O número reduzido de queixas pode ser explicado pelo facto de as competências do Painel se limitarem, tal como acima referido, a um determinado tipo de dados.

O limitado volume de *dossiês* apresentados ao Painel também se poderá explicar, em parte, pelo desconhecimento da existência desta entidade. Desde 2004, a Comissão Europeia tem dado uma maior visibilidade no seu sítio *Web* às informações relativas ao Painel[43].

Para que o Painel seja utilizado de forma mais eficiente, as empresas estabelecidas nos EUA que tenham decidido cooperar com o Painel e dar cumprimento às suas decisões, tanto no que respeita à totalidade como a certas categorias apenas de dados pessoais abrangidos pelas autocertificações respetivas, devem indicar, de forma clara e bem visível nos compromissos

42 «U.S.-EU Cooperation to Implement the Safe Harbor Framework», 12 de novembro de 2013.

43 Em conformidade com o relatório de 2004, foi publicado no sítio *Web* da Comissão (DG Justiça) um aviso de informação sob a forma de perguntas e respostas redigidas pelo Painel sobre a proteção dos dados da UE, com o objetivo de sensibilizar os cidadãos e de os ajudar a apresentar queixas caso considerem que os seus dados pessoais foram tratados em violação do sistema «porto seguro»: http://ec.europa.eu/justice/policies/privacy/docs/adequacy/information_Safe_harbour_en.pdf
O formulário de apresentação das queixas está disponível no sítio:http://ec.europa.eu/justice/policies/privacy/docs/adequacy/complaint_form_en.pdf

assumidos no âmbito das suas políticas de proteção da vida privada que autorizam o Department of Commerce a controlar este aspeto. Deverá ser criada uma página especial sobre o sistema «porto seguro» no sítio *Web* de cada uma das autoridades de proteção de dados da UE, com vista a dar a conhecer melhor este sistema às empresas europeias e às pessoas cujos dados são tratados.

5.3. Melhoria da aplicação coerciva

As deficiências a nível da transparência e da aplicação coerciva identificadas acima preocupam as empresas europeias quanto ao impacto negativo que o sistema de «porto seguro» pode ter na sua competitividade. Quando uma empresa europeia entra em concorrência com uma empresa americana que exerce as suas atividades no âmbito do sistema de «porto seguro», mas que, na prática, não aplica os seus princípios, a empresa europeia sofre de uma desvantagem competitiva em relação à empresa americana.

Além disso, a competência da Comissão Federal do Comércio inclui os atos e as práticas desleais ou fraudulentas «no domínio do comércio». A Secção 5 da Federal Trade Commission Act (lei sobre a Comissão Federal do Comércio) prevê exceções a esta competência no que se refere, nomeadamente, ao domínio das **telecomunicações**. Como não estão abrangidas pelo âmbito de ação da Comissão Federal do Comércio, as empresas de telecomunicações não estão autorizadas a aderir aos princípios de «porto seguro». No entanto, com a crescente convergência das tecnologias e serviços, muitos dos seus concorrentes diretos no setor americano das TIC aderem ao sistema «porto seguro». A exclusão das empresas de telecomunicações do intercâmbio de dados no âmbito do sistema de «porto seguro» é uma questão que preocupa alguns operadores de telecomunicações europeus. De acordo com a Associação dos Operadores Europeus de Redes de Telecomunicações (ETNO), «esta situação é manifestamente contrária às aspirações mais importantes dos operadores de telecomunicações, que salientam a necessidade de garantir uma igualdade de condições para todos[44].

6. REFORÇO DOS PRINCÍPIOS DE «PORTO SEGURO» RELATIVOS À PROTEÇÃO DA VIDA PRIVADA

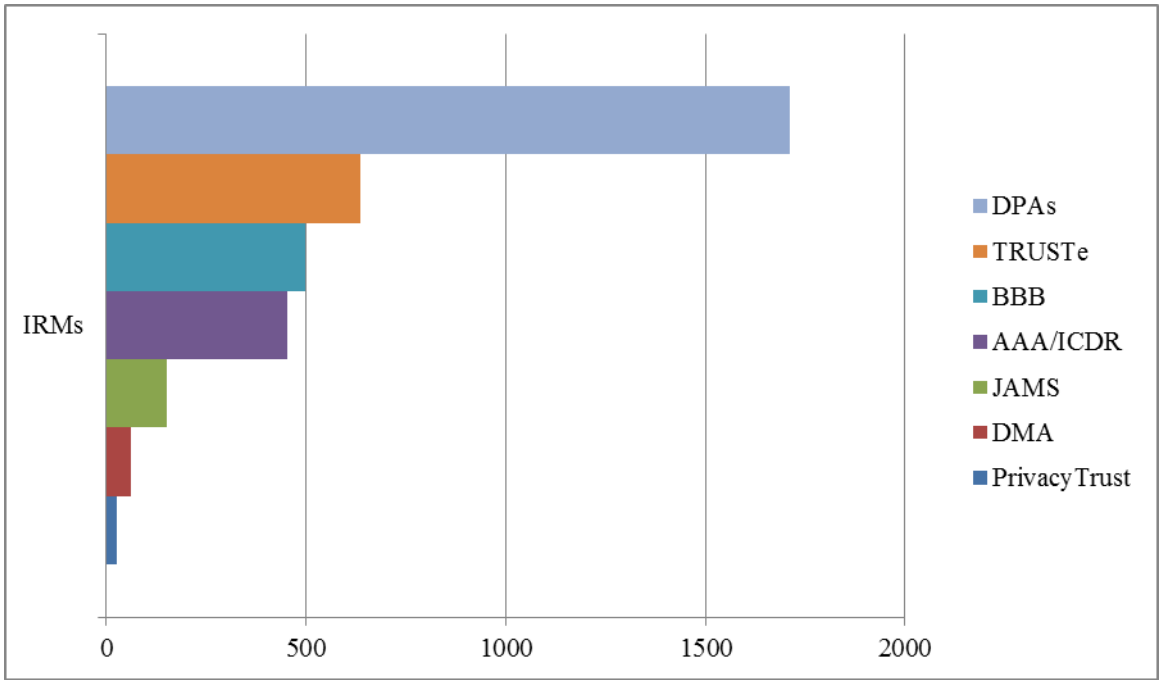
6.1. Resolução alternativa de litígios

O princípio de aplicação requer a existência de «**«mecanismos de recurso imediatamente disponíveis e acessíveis** que permitam investigar as queixas e os litígios apresentados por pessoas singulares». Para esse efeito, o sistema «porto seguro» instaura um sistema de resolução alternativa de litígios (RAL) por um terceiro independente [45] para oferecer aos cidadãos soluções rápidas. Os três principais organismos dotados de mecanismos de recurso são o Painel de proteção de dados da UE, os gabinetes de ética comercial (BBB) e o TRUSTe.

---

44 As «Considerações ETNO» recebidas em 4 de outubro de 2013 pelos serviços da Comissão abordam igualmente 1) a definição de «dados pessoais» no âmbito do sistema «porto seguro» ; 2) o controlo insuficiente do sistema; 3) e o facto de as «empresas americanas poderem transferir dados com muito menos restrições que as aplicáveis aos seus homólogos europeus», o que «constitui uma discriminação manifesta em relação às empresas europeias e afeta a sua competitividade». Em conformidade com as regras de «porto seguro», para poderem divulgar informações a terceiros, as organizações devem obrigatoriamente aplicar os princípios de aviso e de escolha. Se desejarem transferir informações para terceiros que desempenhem a função de agentes, as organizações só o poderão fazer na condição de se certificarem de que o terceiro em questão subscreve os princípios de «porto seguro», cumpre as disposições da diretiva ou outras disposições adequadas, e de estabelecerem um acordo escrito com esse terceiro, exigindo que este garanta, pelo menos, o mesmo nível de proteção da vida privada que o requerido pelos princípios pertinentes.

45 A Diretiva 2013/11/UE sobre a resolução alternativa de litígios de consumo salienta a importância de procedimentos independentes, imparciais, transparentes, eficazes, céleres e equitativos de resolução de litígios.



O recurso à RAL tem vindo a aumentar desde 2004 e o Department of Commerce reforçou a vigilância das entidades de RAL americanas para garantir que as informações que fornecem sobre os procedimentos de recurso sejam claras, acessíveis e compreensíveis. No entanto, a eficácia deste sistema continua por demonstrar devido ao número limitado de casos tratados até à data[46].

Embora o Department of Commerce tenha conseguido reduzir as taxas cobradas por sete grandes entidades RAL, duas das principais entidades neste domínio continuam a cobrar taxas a particulares que apresentam queixa[47]. Trata-se de entidades RAL cujos serviços são utilizados por cerca de 20 % das empresas aderentes ao sistema «porto seguro». Estas empresas selecionaram uma entidade RAL que cobra uma taxa aos clientes para apresentarem queixa. Estas práticas não são conformes com o princípio de aplicação do «porto seguro» que confere aos particulares o direito de aceder a mecanismos de recurso independentes «imediatamente disponíveis e acessíveis». Na União Europeia, o acesso a um serviço de resolução de litígios independente, prestado pelo Painel de proteção dos dados da UE, é gratuito para todos os titulares de dados.

46 A título de exemplo, uma importante entidade («TRUSTe») indicou que dos 881 pedidos que recebera em 2010 só três tinham sido considerados admissíveis e fundamentados, pelo que a empresa em questão foi convidada a modificar a sua política de proteção da vida privada no seu sítio *Web*. Em 2011, o número de queixas elevou-se a 879 , tendo, num caso, a empresa sido convidada a modificar a sua política de proteção da vida privada. Segundo o Department of Commerce, a grande maioria das queixas apresentadas no âmbito da RAL proveem dos consumidores, por exemplo, utilizadores que se esqueceram da sua senha e não a conseguiram recuperar junto do serviço da Internet. A pedido da Comissão, o Department of Commerce desenvolveu novos critérios de comunicação de estatísticas que deverão ser utilizados por todas as RAL. Estes critérios estabelecem uma distinção entre pedidos e queixas e, por outro lado, fornecem esclarecimentos suplementares sobre os tipos de queixas recebidas. No entanto, estes novos critérios deverão ser objeto de um debate mais aprofundado que permita assegurar que as novas estatísticas em 2014 abranjam todas as entidades RAL, sejam comparáveis e forneçam informações determinantes para avaliar a eficácia do mecanismo de recurso.

47 O International Centre for Dispute Resolution/American Arbitration Association (ICDR/AAA) cobra, respetivamente, 200 e 250 dólares US por «despesas administrativas». O Department of Commerce informou a Comissão que tinha trabalhado com a AAA, a entidade de resolução de litígios para particulares mais onerosa, com vista a conceber um programa específico para o sistema «porto seguro» destinado a reduzir os custos para os consumidores de vários milhares de dólares para uma taxa fixa de 200 dólares US.

Em 12 de novembro de 2013, o Department of Commerce confirmou que «continuaria a defender o direito dos cidadãos da UE à proteção da sua vida privada e que estudaria com as entidades RAL as possibilidades de reduzir ainda mais as suas taxas».

No que diz respeito às sanções, nem todas as entidades RAL dispõem dos instrumentos necessários para resolver as situações de desrespeito dos princípios de proteção da vida privada. Além disso, a publicação de casos de incumprimento destes princípios não parece estar prevista entre o leque de sanções e de medidas aplicáveis por todas as entidades RAL.

As entidades RAL são igualmente convidadas a submeter à Comissão Federal do Comércio os casos de empresas que não cumpram as decisões dos processos de RAL ou que rejeitem a decisão das entidades RAL, para que a referida Comissão possa proceder a um exame e a um inquérito e, se for caso disso, adotar medidas coercitivas. No entanto, até à data, as entidades RAL ainda não submeteram casos desse tipo à Comissão Federal do Comércio[48].

As entidades RAL publicam, nos seus sítios *Web*, listas das empresas (participantes em processos de resolução de litígios) que recorrem aos seus serviços, o que permite aos consumidores verificar facilmente — em caso de litígio com uma empresa — se um particular pode apresentar queixa junto de uma determinada entidade RAL. Assim, por exemplo, a entidade RAL «BBB» elabora a lista de todas as empresas abrangidas pelo sistema de resolução alternativa de litígios do seu gabinete. No entanto, um grande número de empresas alegam estar abrangidas por um determinado sistema de resolução de litígios, mas as entidades RAL não as designam como participantes no seu sistema[49].

Os mecanismos de RAL devem ser de acesso fácil, independentes e abordáveis em termos económicos para as pessoas singulares. Um titular de dados deve poder apresentar uma queixa sem que lhe sejam impostas restrições excessivas. Todos os organismos de RAL devem publicar nos seus sítios *Web* estatísticas sobre as queixas apresentadas e tratadas, bem como informações específicas sobre os respetivos resultados. Por último, os organismos de RAL devem ser sujeitos a um controlo posterior destinado a garantir que as informações que facultam acerca do processo e das modalidades de apresentação das queixas sejam claras e compreensíveis, a fim de tornar a resolução dos litígios num mecanismo eficaz, com resultados fiáveis. Importa também reiterar que a publicação de casos de incumprimento deve figurar entre as sanções obrigatórias dos mecanismos de RAL.

6.2. Retransferência

Com o crescimento exponencial do fluxos de dados, é igualmente necessário assegurar a proteção continuada dos dados pessoais em todas as fases do respetivo tratamento, nomeadamente quando uma empresa que tenha subscrito os princípios de «porto seguro» transfere estes dados para um **terceiro que seja subcontratante**. Por conseguinte, a necessidade de assegurar um maior cumprimento do sistema de «porto seguro» diz respeito não só aos aderentes, mas também aos subcontratantes.

Se desejar transferir informações para terceiros que desempenhem a função de agentes, a empresa – membro do sistema «porto seguro» - só o poderá fazer na condição de se certificar de que a parte terceira subscreve os princípios de «porto seguro», cumpre as disposições da diretiva ou outras disposições adequadas, e de estabelecer um acordo escrito com esse

48 Ver FAQ 11.

49 Exemplos: A Amazon informou o Department of Commerce que recorria ao BBB enquanto entidade RAL, mas a BBB não inclui a Amazon na lista dos participantes no seu sistema de RAL. Pelo contrário, a Arsalon Technologies (www.arsalon.net), um fornecedor de serviços de computação na nuvem, figura na lista de RAL da BBB no âmbito do sistema de «porto seguro», embora atualmente essa empresa não seja membro desse sistema (situação em 1 de outubro de 2013). BBB, TRUSTe e outras entidades RAL devem eliminar as declarações de certificação erradas ou corrigi-las. Deverão ficar vinculadas pela condição obrigatória de só certificar as empresas que são efetivamente membros do sistema de «porto seguro».

terceiro, exigindo que este garanta, pelo menos, o mesmo nível de proteção da vida privada que o requerido pelos princípios pertinentes» [50]. [51]Por exemplo, um fornecedor de serviços de computação em nuvem é convidado pelo Department of Commerce a celebrar um contrato mesmo que cumpra os princípios de «porto seguro» e receba dados pessoais para tratamento. Todavia, esta disposição não é clara no anexo II da Decisão «porto seguro».

Como o recurso a subcontratantes aumentou consideravelmente nos últimos anos, em especial no contexto da computação em nuvem, quando é celebrado um contrato, uma empresa membro do sistema de «porto seguro» deve desse facto notificar o Department of Commerce e publicar as suas garantias em matéria de proteção da vida privada[52].

Os três elementos acima referidos, a saber, o mecanismo de resolução alternativa de litígios, o reforço da supervisão e a retransferência de dados, deverão ser clarificados.

7. ACESSO A DADOS TRANSFERIDOS NO ÂMBITO DO SISTEMA DE «PORTO SEGURO»

Em 2013, as informações sobre a dimensão e o âmbito dos programas de vigilância dos EUA suscitaram grandes preocupações sobre a continuação da proteção de dados pessoais legalmente transferidos para os Estados Unidos ao abrigo do sistema de «porto seguro». Por exemplo, todas as empresas que participam no Programa PRISM, que permite às autoridades americanas ter acesso a dados armazenados e tratados nos EUA, parecem estar certificadas no âmbito do sistema de «porto seguro». Este sistema passou, pois, a ser uma das vias através da qual os serviços de informações americanos têm acesso à recolha de dados pessoais inicialmente tratados na UE.

A Decisão «porto seguro» prevê, no seu anexo I, que a adesão aos princípios de proteção da vida privada pode ser limitada para observar requisitos de segurança nacional, interesse público ou execução legal, de legislação, regulamento governamental ou jurisprudência. Para serem válidas, as limitações e restrições ao exercício dos direitos fundamentais devem ser interpretadas de forma restritiva; devem ser enunciadas numa legislação acessível ao público e necessárias e proporcionadas numa sociedade democrática. Em especial, a Decisão «porto seguro» especifica que essas limitações são permitidas apenas **«na medida necessária»** para observar requisitos de segurança nacional, interesse público ou execução legal[53]. Embora o tratamento excecional de dados para fins de segurança nacional, interesse público ou execução legal esteja previsto no sistema de «porto seguro», quando este sistema foi adotado

50 Ver Decisão da Comissão 2000/520/CE, página 7 (Retransferência).

51 Ver: «Clarifications Regarding the U.S.-EU Safe Harbor Framework and Cloud Computing»: http://export.gov/static/Safe%20Harbor%20and%20Cloud%20Computing%20Clarification_April%2012%202013_Latest_eg_main_060351.pdf

52 Estas observações dizem respeito aos fornecedores de serviços de computação em nuvem que não são membros do sistema de «porto seguro». De acordo com a empresa de consultoria Galexia, «o nível de adesão e de cumprimento («porto seguro») entre este tipo de prestadores de serviços é bastante elevado. Em geral, têm vários níveis de proteção da vida privada, combinando muitas vezes contratos diretos com os clientes com políticas globais em matéria de proteção da vida privada. Com uma ou duas exceções importantes, estes prestadores de serviços no âmbito do sistema de «porto seguro» respeitam as principais disposições em matéria de resolução de litígios e respetiva aplicação. Atualmente, na lista das empresas que prestaram declarações de adesão falsas não figura nenhum fornecedor de serviços de computação em nuvem.» (Intervenção de Chris Connolly da Galexia no inquérito da Comissão LIBE sobre a vigilância maciça eletrónica dos cidadãos da UE).

53 Ver anexo 1 da Decisão «porto seguro»: A adesão a estes princípios pode ser limitada: a) na medida necessária para observar requisitos de segurança nacional, interesse público ou execução legal, b) por legislação, regulamento governamental ou jurisprudência que criam obrigações contraditórias ou autorizações explícitas, desde que, no exercício de tal autorização, uma organização possa demonstrar que o seu incumprimento dos princípios se limita ao necessário para respeitar os legítimos interesses superiores avançados por essa autorização, ou c) por exceção ou derrogação prevista na diretiva ou nas normas de direito interno dos Estados-Membros, desde que a aplicação das referidas exceções ou derrogações ocorra em contextos comparáveis. Para que se possa melhorar a proteção da vida privada, as organizações deverão envidar esforços no sentido de aplicar estes princípios de forma integral e transparente, incluindo a indicação das respetivas políticas de proteção da vida privada, sempre que as exceções aos princípios permitidas pela alínea b) supra se apliquem regularmente. Pela mesma razão, quando a escolha for permitida pelos princípios e/ou pela legislação norte-americana, as organizações deverão optar pelo nível de proteção mais elevado possível».

não era possível prever o acesso em grande escala por parte dos serviços de informações aos dados transferidos para os Estados Unidos no âmbito de transações comerciais.

Além disso, por motivos de transparência e de segurança jurídica, a Comissão Europeia deve ser notificada pelo Department of Commerce de qualquer texto legislativo ou regulamento governamental que afete a adesão aos princípios de «porto seguro»[54]. O recurso às derrogações deverá ser cuidadosamente controlado, não devendo estas ser utilizadas de forma que comprometa a proteção assegurada pelos **princípios de «porto seguro»**[55]**.** Em especial, o acesso em larga escala pelas autoridades dos EUA aos dados tratados pelas empresas autocertificadas «porto seguro» pode comprometer a confidencialidade das comunicações eletrónicas.

7.1. Proporcionalidade e necessidade

Segundo as conclusões do Grupo de trabalho *ad hoc* UE-EUA em matéria de proteção de dados, uma série de bases jurídicas previstas pela legislação americana permitem recolher e tratar em grande escala dados pessoais, que são armazenados ou tratados por empresas estabelecidas nos EUA. Tal pode incluir dados transferidos anteriormente da UE para os EUA no âmbito do sistema de «porto seguro», o que levanta a questão da interrupção do cumprimento dos princípios de «porto seguro». Como se trata de programas de grande envergadura, é possível que os dados transferidos no âmbito do sistema de «porto seguro» sejam acessíveis às autoridades americanas e sejam por estas tratados para além do estritamente necessário e proporcional em relação à proteção da segurança nacional, como previsto na derrogação enunciada na Decisão «porto seguro».

7.2. Limitações e possibilidades de recurso

Segundo as conclusões do grupo de trabalho *ad hoc* UE-EUA em matéria de proteção de dados, são sobretudo os cidadãos dos EUA ou os residentes legais que beneficiam das salvaguardas fornecidas ao abrigo da legislação americana. Além disso, não existe qualquer possibilidade de os titulares de dados da UE ou dos EUA obterem acesso ou solicitarem a retificação ou a supressão dos dados, ou apresentarem um recurso administrativo ou judicial caso, no âmbito de programas de vigilância dos EUA, os seus dados pessoais sejam recolhidos e tratados posteriormente.

7.3. Transparência

As empresas não indicam sistematicamente, nas suas políticas de proteção da vida privada, em que casos aplicam exceções ao sistema de «porto seguro». Os particulares e as empresas não têm, pois, conhecimento da utilização que é feita dos seus dados, o que é especialmente relevante no que respeita à exploração dos programas de vigilância americanos em questão. Por conseguinte, os europeus cujos dados são transferidos para uma empresa estabelecida nos EUA que aderiu ao sistema de «porto seguro» podem não ser informados por essa empresa de que o acesso aos seus dados é possível[56]. Esta situação levanta a questão do cumprimento dos

---

54 Parecer n. °4/2000 sobre o nível de proteção assegurado pelos princípios de «porto seguro» adotado, em 16 de maio de 2000, pelo grupo de trabalho criado nos termos do artigo 29.º.

55 Parecer n.° 4/2000 sobre o nível de proteção assegurado pelos princípios de «porto seguro» adotado, em 16 de maio de 2000, pelo grupo de trabalho criado nos termos do artigo 29.º.

56 Algumas empresas que participam no sistema de «porto seguro» fornecem informações relativamente transparentes a este respeito. A Nokia, por exemplo, que está estabelecida nos EUA e é membro do sistema de «porto seguro», fornece a seguinte informação sobre a sua política de proteção da vida privada: «*Podemos ser legalmente obrigados a divulgar os seus dados*

princípios de «porto seguro» em matéria de transparência, a qual deve ser assegurada tanto quanto possível, sem comprometer a segurança nacional. Para além de, como previsto atualmente, terem a obrigação de indicar nas suas políticas de proteção da vida privada os casos em que os princípios podem ser limitados pela legislação, regulamento governamental ou jurisprudência, as empresas devem também ser encorajadas a indicar, nas suas políticas de proteção da vida privada, as situações em que aplicam exceções aos princípios de «porto seguro» para observar requisitos de segurança nacional, interesse público ou execução legal.

8. CONCLUSÕES E RECOMENDAÇÕES

Desde que foi adotado em 2000, o sistema «porto seguro» tornou-se um vetor para o fluxo de dados pessoais entre a UE e os EUA. A importância de dispor de uma proteção eficaz no caso de transferências de dados pessoais tem vindo a aumentar devido ao aumento exponencial dos fluxos de dados, cruciais para a economia digital, bem como aos enormes progressos realizados a nível da recolha, do tratamento e da utilização dos dados. As empresas da Internet como a Google, Facebook, Microsoft, Apple e Yahoo, possuem centenas de milhões de clientes na Europa e transferem dados pessoais destinados a ser tratados nos EUA numa escala impensável no ano 2000.

As deficiências verificadas a nível da transparência e da aplicação do acordo contribuem para perpetuar os seguintes problemas específicos, que deverão ser abordados:

(a) Transparência das políticas de proteção da vida privada adotadas pelos membros do sistema «porto seguro»,

(b) Aplicação efetiva dos princípios de proteção da vida privada pelas empresas nos EUA e

(c) Eficácia da sua aplicação.

Além disso, o **acesso em grande escala pelos serviços de informações a dados transferidos para os EUA por empresas certificadas participantes no sistema de «porto seguro»** levanta novas questões graves sobre a continuidade dos direitos dos cidadãos europeus em matéria de proteção de dados quando os seus dados pessoais são transferidos para os EUA.

Com base no que precede, a Comissão formula as seguintes **recomendações**:

Transparência

(1) *As empresas autocertificadas devem divulgar publicamente as suas políticas de proteção da vida privada*. Não basta que forneçam ao Department of Commerce uma descrição das suas políticas em matéria de proteção da vida privada. Estas devem ser disponibilizadas ao público nas páginas *Web* das respetivas empresas e formuladas de forma clara e compreensível.

(2) As políticas de proteção da vida privada publicadas nos sítios Web das empresas autocertificadas devem incluir sistematicamente uma ligação para o sítio Web «porto seguro» do Department of Commerce, no qual deve figurar uma lista dos membros atuais do sistema. Os titulares de dados europeus poderão assim verificar imediatamente, sem buscas adicionais, se uma determinada empresa é, nesse momento, membro do sistema de «porto seguro». Tal contribuirá para reforçar a credibilidade do sistema, graças à diminuição das possibilidades de declarações

---

pessoais a certas autoridades ou a outros terceiros, por exemplo, às autoridades responsáveis pela aplicação coerciva da lei, nos países em que estamos presentes ou em que estão presentes terceiros que agem em nosso nome.»

falsas de adesão aos princípios de «porto seguro». Em março de 2013, o Department of Commerce começou a impor esta exigência às empresas, mas este processo deverá ser intensificado.

(3) As empresas autocertificadas devem publicar as condições de proteção da vida privada de quaisquer contratos que celebrarem com os subcontratantes, por exemplo, os serviços de computação em nuvem. O sistema de «porto seguro» autoriza as retransferências das empresas autocertificadas participantes neste sistema para terceiros que agem como «agentes», por exemplo, os fornecedores de serviços de computação em nuvem. Tanto quanto é do nosso conhecimento, o Department of Commerce exige que as empresas autocertificadas celebrem um contrato. No entanto, quando celebram um contrato desse tipo, as empresas participantes no sistema de «porto seguro» devem igualmente informar desse facto o Department of Commerce e ser obrigadas a tornar públicas as salvaguardas que oferecem em matéria de proteção da vida privada.

(4) *Indicação clara, no sítio Web do Department of Commerce, de todas as empresas que não são membros atuais do regime*. O estatuto «não atual» constante da lista dos membros do sistema «porto seguro» do Department of Commerce deve ser acompanhado de um aviso claro de que, nesse momento, a empresa correspondente não cumpre os requisitos do sistema de «porto seguro». No entanto, caso o estatuto da empresa seja «não atual», esta deve, mesmo assim, continuar a aplicar os requisitos do sistema de «porto seguro» relativamente a dados que tenha recebido no âmbito desse sistema.

Recurso

(5) As políticas de proteção da vida privada publicadas nos sítios Web das empresas devem incluir uma ligação para o sítio Web da entidade responsável pela resolução alternativa de litígios (RAL) e/ou do Painel de proteção de dados da UE. Tal permitirá aos titulares de dados europeus contactar imediatamente a entidade RAL ou o Painel de proteção de dados da UE em caso de problemas. Em março de 2013, o Department of Commerce começou a impor esta exigência às empresas, mas este processo deverá ser intensificado.

(6) *As entidades RAL devem ser facilmente acessíveis e pouco onerosas*. Algumas das entidades RAL que aderiram ao sistema de «porto seguro» continuam a cobrar taxas a particulares — que podem ser bastante onerosas— pelo processamento de uma queixa (entre 200 e 250 dólares US). Em contrapartida, na Europa o acesso ao Painel de proteção dos dados da UE previsto para a resolução das queixas respeitantes ao sistema «porto seguro» é gratuito.

(7) O Department of Commerce deverá controlar de forma mais sistemática as entidades RAL em termos da sua transparência e da acessibilidade das informações que fornecem sobre o processo utilizado e o seguimento dado às queixas que lhes são apresentadas. Tal tornará a resolução de litígios num mecanismo eficaz e fiável, que produz efetivamente resultados. Importa também lembrar que a publicação de casos de incumprimento deve ser incluída no leque de sanções obrigatórias das entidades RAL.

Aplicação

(8) Na sequência da certificação ou da recertificação de empresas no âmbito do sistema «porto seguro», uma percentagem dessas empresas deve ser sujeita a inquéritos

sistemáticos sobre o cumprimento efetivo das respetivas políticas de proteção da vida privada (para além do controlo do cumprimento das exigências formais).

(9) Sempre que seja constatado um caso de incumprimento, na sequência de uma queixa ou de um inquérito, a empresa em causa deve ser objeto, um ano depois, de um inquérito específico.

(10) Caso existam queixas pendentes ou dúvidas quanto ao cumprimento dos princípios de «porto seguro», por parte de uma empresa, o Department of Commerce deve informar a autoridade competente da UE em matéria de proteção de dados.

(11) *As declarações falsas de adesão ao sistema de «porto seguro» devem continuar a ser investigadas.* Uma empresa que afirma no seu sítio *Web* que cumpre os requisitos do sistema «porto seguro», mas que não figura na lista do Department of Commerce na qualidade de membro «atual» induz em erro os consumidores e abusa da sua confiança. As declarações falsas enfraquecem a credibilidade geral do sistema, pelo que devem ser imediatamente retiradas dos sítios *Web* das empresas.

Acesso pelas autoridades dos EUA

(12) As 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.

(13) É importante que a exceção por motivos de segurança nacional prevista na Decisão «porto seguro» seja utilizada apenas de forma proporcional e na medida em que for estritamente necessária.