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 assegurado pelos princípios de «porto seguro» e pelas respectivas questões mais frequentes (FAQ) emitidos pelo Department of Commerce dos Estados Unidos da América

[notificada com o número C(2000) 2441]

(Texto relevante para efeitos do EEE)

(2000/520/CE)

A COMISSÃO DAS COMUNIDADES EUROPEIAS,

Tendo em conta o Tratado que institui a Comunidade Europeia,

Tendo em conta a 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 [1], e, nomeadametne, o n.º 6 do seu artigo 25.º,

Considerando o seguinte:

(1) Nos termos da Directiva 95/46/CE, os Estados-Membros devem prever que a transferência de dados pessoais para um país terceiro só pode realizar-se se o país terceiro em questão assegurar um nível de protecção adequado e a lei de execução dos Estados-Membros de outras disposições da directiva tiver sido respeitada antes de efectuada a transferência.

(2) A Comissão pode determinar se um país terceiro garante um nível de protecção adequado. Nesse caso podem ser transferidos dados pessoais a partir dos Estados-Membros sem que sejam necessárias garantias adicionais.

(3) Nos termos da directiva, a adequação do nível de protecção de dados deve ser apreciada em função de todas as circunstâncias que acompanham a operação de transferência de dados ou o conjunto de operações de transferência de dados, com relação a determinadas regras. O grupo de trabalho «Protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais», criado pela referida directiva [2] estabeleceu directrizes para efectuar tal apreciação [3].

(4) Dados os diferentes níveis de protecção nos países terceiros, o nível de adequação da protecção de dados deve ser apreciado e quaisquer decisões com base no n.º 6 do artigo 25.º devem ser aplicadas de forma que não se verifique uma discriminação arbitrária ou injustificada contra ou entre países terceiros, onde prevaleçam condições semelhantes, nem um obstáculo dissimulado ao comércio, tendo em conta os actuais compromissos internacionalmente assumidos pela Comunidade.

(5) O nível adequado de protecção da transferência de dados a partir da Comunidade Europeia para os Estados Unidos da América (EUA), nos termos da presente decisão, pode conseguir-se se as organizações derem cumprimento aos princípios da «privacidade em porto seguro» relativos à protecção de dados pessoais transferidos de um Estado-Membro para os EUA (a seguir denominados «os princípios») e às directrizes das questões mais frequentes (a seguir designadas «FAQ») que servem de guia no que respeita à aplicação dos princípios estabelecidos pelo Governo dos Estados Unidos em 21 de Julho de 2000. Por outro lado, as organizações devem dar a conhecer publicamente as suas políticas em matéria de protecção da vida privada e ficar abrangidas pelo âmbito da competência da Federal Trade Comission (FTC) que, nos termos do artigo 5.º da lei relativa ao comércio federal (Section 5 of the Federal Trade Commission Act), garante a proibição dos actos ou as práticas desleais ou enganosas relativas ao comércio, ou de outros organismos públicos que efectivamente assegurem o respeito dos princípios aplicados em conformidade com as FAQ.

(6) Os sectores e/ou tratamento de dados não incluídos no âmbito da competência dos órgãos administrativos dos Estados Unidos da América referidos no anexo VII da presente decisão não são por ela abrangidos.

(7) A fim de garantir a correcta aplicação da presente decisão, é necessário que as organizações que aderirem ao conjunto de princípios e às FAQ sejam reconhecidas pelos interessados directos, tais como pessoas cujos dados foram objecto de tratamento, exportadores de

---

[1] JO L 281 de 23.11.1995, p. 31.

[2] Endereço *web* do grupo de trabalho: http://www.europa.eu.int/comm/internal_market/en/media/dataprot//wpdocs/index.htm

[3] WP 12: transferência de dados pessoais para países terceiros: aplicação dos artigos 25.º e 26.º da directiva comunitária sobre protecção de dados, documento adoptado pelo grupo de trabalho em 24 de Julho de 1998.

dados e entidades responsáveis pela protecção dos dados. Para o efeito o US Department of Commerce, ou um seu representante, assumirá a responsabilidade de manter actualizada uma lista pública das organizações que aderirem ao referido conjunto de princípios aplicados segundo as orientações das FAQ e que estejam abrangidos pelo âmbito de competência de, pelo menos, uma das entidades públicas referidas no anexo VII da presente decisão.

(8) Num interesse de transparência e para salvaguardar a capacidade de as autoridades competentes nos Estados-Membros assegurarem a protecção das pessoas no que diz respeito ao tratamento de dados pessoais, é necessário precisar na presente decisão as circunstâncias excepcionais em que a suspensão de fluxos concretos de dados se pode justificar, apesar de verificado um nível de protecção adequado.

(9) O «porto seguro» criado pelos princípios e pelas FAQ pode necessitar de revisão à luz da experiência dos desenvolvimentos relativos à protecção da vida privada em circunstâncias em que a tecnologia torna cada vez mais fáceis a transferência e o tratamento de dados pessoais e à luz de relatórios relativos à aplicação dada pelas entidades responsáveis.

(10) Os pareceres emitidos pelo grupo de trabalho «Protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais», criado pelo artigo 29.º da Directiva 95/46/CE, sobre o nível de protecção facultado pelos princípios de «porto seguro» nos EUA, foram tidos em conta na preparação da presente decisão [4].

(11) As medidas previstas pela presente decisão estão em conformidade com o parecer do comité estabelecido pelo artigo 31.º da Directiva 95/46/CE,

[4] WP 15: Parecer 1/99 relativo ao nível de protecção dos dados nos Estados Unidos e às negociações em curso entre a Comissão Europeia e o Governo dos Estados Unidos.
WP 19: Parecer 2/99 sobre a adequação dos «International Safe Harbor Principles» (princípios internacionais de porto seguro) enunciados pelo Departamento de Comércio dos EUA em 19 de Abril de 1999.
WP 21: Parecer 4/99 sobre as questões mais frequentes a publicar pelo Departamento de Comércio dos EUA no quadro da proposta de princípios de «porto seguro».
WP 23: Documento de trabalho sobre o avanço das negociações entre a Comissão Europeia e o Governo dos Estados Unidos da América relativas aos «princípios internacionais de porto seguro».
WP 27: Parecer 7/99 sobre o nível de protecção de dados fornecido pelos princípios de «porto seguro», publicados em conjunto com as questões mais frequentes (FAQ) e outros documentos conexos, em 15 e 16 de Novembro de 1999, pelo Department of Commerce dos EUA.
WP 31: Parecer 3/2000 relativo ao diálogo UE/EUA sobre o Acordo de «porto seguro».
WP 32: Parecer 4/2000 relativo ao nível de protecção facultado pelos acordos de «porto seguro».

ADOPTOU A PRESENTE DECISÃO:

Artigo 1.º

1. Nos termos do n.º 2 do artigo 25.º da Directiva 95/46/CE, para efeitos de todas as actividades abrangidas pelo âmbito da directiva, considera-se que os «princípios da privacidade em porto seguro» (a seguir denominados «os princípios») que figuram no anexo I da presente decisão, aplicados em conformidade com a orientação que proporcionam as questões mais frequentes (a seguir designadas «FAQ»), publicadas pelo Department of Commerce dos EUA, em 21 de Julho de 2000 que figuram no anexo II da presente decisão, asseguram um nível adequado de protecção dos dados pessoais transferidos a partir da Comunidade Europeia para organizações estabelecidas nos Estados Unidos da América, tendo em conta os seguintes documentos emanados do Department of Commerce dos EUA:

a) O resumo global de aplicação dos princípios de porto seguro que figura no anexo III;

b) O memorando sobre danos por violação das regras de protecção da vida privada e autorizações explícitas previstas na lei dos EUA, que figura no anexo IV;

c) O ofício da Federal Trade Commission que figura no anexo V;

d) O ofício do Department of Transportation que figura no anexo VI.

2. No que respeita a cada transferência de dados:

a) A organização destinatária dos dados comprometer-se-á clara e publicamente a cumprir os princípios aplicados em conformidade com as FAQ; e

b) A referida organização fica sujeita aos poderes legais dos entes públicos administrativos norte-americanos referidos no anexo VII da presente decisão, com competência para investigar denúncias, tomar medidas contra práticas desleais e enganosas, assim como proceder à reparação de pessoas singulares, independentemente do seu país de residência ou da sua nacionalidade, sempre que se verificar incumprimento dos princípios segundo as orientações das FAQ.

3. Considera-se que a organização que declarar a sua adesão aos princípios aplicados em conformidade com as FAQ cumpre o disposto no n.º 2, a partir da data em que comunicar ao Department of Commerce dos EUA ou ao seu representante, a divulgação do compromisso referido na alínea a) do n.º 2, bem como a identidade da entidade pública a que se refere a alínea b) do n.º 2.

Artigo 2.º

A presente decisão diz respeito tão só ao nível adequado de protecção previsto nos Estados Unidos da América nos termos dos princípios aplicados nos termos da FAQ a fim de dar cumprimento ao disposto no n.º 1 do artigo 25.º da Directiva 95/46/CE e não prejudica a aplicação de outras disposições da referida directiva relativas ao tratamento de dados pessoais nos Estados-Membros e nomeadamente o seu artigo 4.º

Artigo 3.º

1. Sem prejuízo da competência para tomar medidas que garantam o cumprimento das disposições nacionais adoptadas por força de outras disposições além das previstas no artigo 25.º da Directiva 95/46/CE, as autoridades competentes dos Estados-Membros podem exercer as suas competências para suspender a transferência de dados para uma organização que tenha declarado a sua adesão aos princípios aplicados em conformidade com as FAQ, se isso se verificar necessário à protecção das pessoas no que diz respeito ao tratamento dos seus dados pessoais, nos casos seguintes:

a) A entidade pública administrativa norte-americana referida no anexo VII da presente decisão, ou um mecanismo de recurso independente, nos termos da alínea a) do princípio de aplicação que figura no anexo I da presente decisão, determinou que a organização violou os princípios em conformidade com as FAQ; ou

b) Existem fortes probabilidades para supor que os princípios não estão a ser respeitados. Há indícios de que o mecanismo de aplicação em causa não toma ou não tomará as medidas adequadas na altura necessária para resolver o caso em questão, que a continuação da transferência dos dados pode causar graves prejuízos às pessoas em causa e que as entidades competentes nos Estados-Membros envidaram esforços razoáveis, dadas as circunstâncias, para facultar à organização em causa a informação e oportunidade necessárias para responder.

A suspensão cessará assim que o respeito dos princípios aplicados em conformidade com as FAQ estiver assegurado e a autoridade competente em questão na Comunidade Europeia seja disso informada.

2. Os Estados-Membros devem informar imediatamente a Comissão da adopção de medidas nos termos do n.º 1.

3. Os Estados-Membros e a Comissão devem ainda manter-se mutuamente informados relativamente aos casos em que os organismos responsáveis pelo cumprimento dos princípios aplicados em conformidade com as FAQ nos Estados Unidos da América não garantam esse mesmo cumprimento.

4. Se a informação recolhida nos termos dos n.ºs 1 a 3 demonstrar que os organismos responsáveis pelo cumprimento dos princípios em conformidade com as FAQ nos Estados Unidos da América não desempenham eficazmente as suas funções, a Comissão deve informar o Department of Commerce norte-americano e, se necessário, apresentar um projecto de medidas, de acordo com o procedimento estabelecido no artigo 31.º da directiva, para revogar ou suspender a presente decisão ou limitar o seu âmbito.

Artigo 4.º

1. A presente decisão pode ser adaptada em qualquer altura, à luz da experiência proporcionada pela sua aplicação e/ou se o nível de protecção proporcionado pelos princípios e pelas FAQ for considerado insuficiente pela lei norte-americana.

Em qualquer caso, a Comissão deve apreciar a aplicação da presente decisão com base na informação disponível, três anos após a sua notificação aos Estados-Membros, e informar o comité estabelecido pelo artigo 31.º da Directiva 95/46/CE de todas as conclusões pertinentes e, nomeadamente, de todas as provas que possam afectar a apreciação da adequação do nível de protecção do disposto no artigo 1.º da presente decisão, nos termos do artigo 25.º da directiva, e de todas as provas de aplicação discriminatória da decisão.

2. A Comissão apresentará, se necessário, projectos de medidas de acordo com o previsto no artigo 31.º da diretiva.

Artigo 5.º

Os Estados-Membros tomarão todas as medidas necessárias para dar cumprimento à presente decisão, o mais tardar até 90 dias após a data da sua notificação aos Estados-Membros.

Artigo 6.º

Os Estados-Membros são os destinatários da presente decisão.

Feito em Bruxelas, em 26 de Julho de 2000.

Pela Comissão

Frederik BOLKESTEIN

Membro da Comissão

ANEXO I

PRINCÍPIOS DE «PORTO SEGURO» (PROTECÇÃO DA VIDA PRIVADA)

emitidos pelo Department of Commerce dos EUA em 21 de Julho de 2000

Em 25 de Outubro de 1998, entrou em vigor a directiva relativa à protecção de dados pessoais, que constitui a legislação geral da União Europeia no domínio da vida privada. Prevê que a transferência de dados pessoais apenas se efectue para os países exteriores à UE que ofereçam garantias de um nível «adequado» de protecção da vida privada. Os Estados Unidos e a União Europeia, embora perfilhem o propósito comum de assegurar a protecção da vida privada dos seus cidadãos, abordam a questão de formas diferentes. Os Estados Unidos recorrem a uma abordagem sectorial com base numa mescla de legislação, regulamentação e auto-regulamentação. Consideradas essas diferenças, muitas organizações dos EUA manifestaram a sua incerteza em relação ao impacto do «padrão de adequação» exigido pela UE no que respeita às transferências de dados pessoais da União Europeia para os Estados Unidos.

Para limitar esta incerteza e fornecer um enquadramento mais previsível para as transferências de dados, o Department of Commerce formula o presente documento e as FAQ, questões mais frequentes (os princípios), nos termos da sua autoridade legal para incentivar, promover e desenvolver o comércio internacional. Os princípios foram desenvolvidos com base em consultas ao sector e ao público em geral para facilitar as relações comerciais e as transacções entre os Estados Unidos e a União Europeia. Destinam-se a ser utilizados exclusivamente por organizações dos EUA que recebam dados pessoais da União Europeia para efeitos de reconhecimento como «porto seguro» e para a presunção de «adequação» implicada nesse processo. Visto que estes princípios foram concebidos com aquele objectivo específico, a sua adopção para outros fins pode revelar-se imprópria. Os princípios não podem ser utilizados em substituição de disposições nacionais de aplicação da directiva em matéria de tratamento de dados pessoais nos Estados-Membros.

A decisão de preencher os requisitos de «porto seguro» é inteiramente voluntária e as organizações podem preencher os requisitos de «porto seguro» de várias formas. As organizações que decidam aderir aos princípios devem agir em conformidade com os mesmos, de modo a obterem e conservarem os benefícios de «porto seguro» e a poderem declará-lo publicamente. Por exemplo, se uma organização se associar a um programa de auto-regulamentação para a protecção da vida privada que adira a estes princípios, preenche os requisitos de «porto seguro». O mesmo se aplica às organizações que desenvolvam as suas próprias políticas auto-reguladoras de protecção da vida privada, desde que ajam em conformidade com os referidos princípios. Quando, para fins do cumprimento dos princípios, uma organização se baseia total ou parcialmente num processo de auto-regulamentação, o seu incumprimento da referida auto-regulamentação poderá ser objecto de recurso, de acordo com o previsto no artigo 5.º da lei relativa ao comércio federal (Section 5 of the Federal Trade Commission Act), que proíbe os actos desleais ou enganosos, ou conforme outra legislação ou regulamentação que proíba esse tipo de actos (ver o anexo com a lista das entidades públicas nos EUA reconhecidas pela UE). Ademais, as organizações regidas por disposições legais, regulamentares, administrativas ou de qualquer outra natureza jurídica que protejam efectivamente a privacidade dos dados pessoais podem candidatar-se aos benefícios do «porto seguro». Em todo o caso, os benefícios do «porto seguro» serão efectivos a partir da data em que a organização que deles deseje usufruir apresente uma autocertificação ao Department of Commerce (ou a um seu representante), de acordo com o estabelecido na FAQ sobre autocertificação.

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 excepção ou derrogação prevista na directiva ou nas normas de direito interno dos Estados-Membros, desde que a aplicação das referidas excepções ou derrogações ocorra em contextos comparáveis. Para que se possa melhorar a protecção da vida privada, as organizações deverão envidar esforços no sentido de aplicar estes princípios de forma integral e transparente, incluindo a indicação das respectivas políticas de protecção da vida privada, sempre que as excepções 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 protecção mais elevado possível.

As organizações poderão, por razões práticas ou outras, aplicar os princípios a todas as operações de tratamento de dados, mas só serão obrigadas a fazê-lo com as transferências de dados posteriores à data de adesão ao «porto seguro». Para preencherem os requisitos de «porto seguro», as organizações não são obrigadas a aplicar estes princípios à informação depositada em sistemas de arquivo tratados manualmente. As organizações que desejam beneficiar do estatuto de «porto seguro» para receberem transferências de informação existente em sistemas de arquivo tratados manualmente proveniente da UE devem aplicar os princípios a qualquer informação desse tipo transferida desde a sua adesão ao

«porto seguro». Uma organização que deseje aplicar os princípios de «porto seguro» a informação pessoal sobre recursos humanos transferida da UE, para utilização no contexto de relações laborais, deve indicá-lo na autocertificação apresentada ao Department of Commerce (ou ao seu representante), em conformidade com o disposto na FAQ sobre autocertificação. Além disso, poderão apresentar as garantias consideradas necessárias pelo artigo 26.º da directiva se incluírem os princípios nos acordos que celebrarem por escrito com as entidades que transferem os dados provenientes da UE como disposições específicas de vida privada, desde que a Comissão e os Estados-Membros autorizem as restantes disposições desses contratos-modelo.

Aplica-se o direito norte-americano às questões de interpretação e respeito dos princípios de «porto seguro» (incluindo as FAQ) e outras medidas de protecção da vida privada praticadas pelas organizações aderentes ao «porto seguro», à excepção de casos em que as organizações se tenham comprometido a cooperar com as entidades europeias responsáveis pela protecção dos dados. Salvo indicação em contrário, nesta matéria são aplicáveis todas as disposições dos princípios de «porto seguro» e das FAQ.

«Dados pessoais» e «informação pessoal» são os dados que se referem a uma pessoa identificada ou identificável, que entrem no âmbito da directiva e que, sendo provenientes da UE, sejam recebidos por entidades norte-americanas, independentemente da forma em que se encontrem registados.

AVISO

Uma organização deve informar os cidadãos quanto aos fins a que se destinam a recolha e utilização dos dados que lhes dizem respeito, à forma de contactar a organização para qualquer questão ou queixa, aos tipos de terceiros a quem a informação é comunicada e às opções e meios que a organização coloca à disposição dos cidadãos para limitarem a utilização e comunicação desses dados. Este aviso deve ser formulado em linguagem clara e de forma bem visível no momento em que se solicita pela primeira vez qualquer informação pessoal aos cidadãos ou então logo que possível, mas, em qualquer circunstância, antes de a organização utilizar esses dados para outro fim diferente daquele que, inicialmente, motivou a recolha ou o tratamento por parte da entidade que procedeu à transferência, ou ainda antes de a organização divulgar, pela primeira vez, esses dados a terceiros [1].

ESCOLHA

Uma organização deve facultar aos cidadãos a possibilidade de escolher («opt out» — opção de não participação) se os seus dados pessoais podem: a) ser divulgados a terceiros [1], ou b) ser utilizados para fins incompatíveis com os que presidiram à recolha inicial ou com os que foram subsequentemente autorizados pela pessoa em causa. Para poderem optar, as pessoas devem ter acesso a mecanismos claros e transparentes, facilmente disponíveis e pouco onerosos.

Para recolha de informações de natureza mais sensível (informações pessoais relativas a condições de saúde ou doenças, origem racial ou étnica, opiniões políticas, crenças religiosas ou filosóficas, pertença a sindicatos ou informações relativas à vida sexual da pessoa), os cidadãos devem poder exercer uma escolha afirmativa ou explícita no sentido da participação («opt in»), caso se pretenda divulgar a informação a terceiros ou utilizá-la para um fim diferente do que, inicialmente, motivou a sua recolha ou do fim subsequentemente autorizado pela pessoa através do exercício da opção de participação. Em qualquer caso, qualquer informação recebida de terceiros, que estes tratem e considerem como sendo de natureza sensível, deverá ser tratada como tal pela organização destinatária.

RETRANSFERÊNCIA

Para poderem divulgar informação a terceiros, as organizações deverão aplicar os princípios de aviso e escolha. Se desejarem transferir informações para terceiros que desempenhem a função de agentes, tal como descrito na nota final, as organizações só o poderão fazer na condição de se certificar de que a parte terceira subscreve os princípios de «porto seguro», cumpre as disposições da directiva ou outras disposições adequadas, e de estabelecer um acordo escrito com esse terceiro, exigindo que este garanta, pelo menos, o mesmo nível de protecção da vida privada requerido pelos princípios pertinentes. Se a organização cumprir estes requisitos, não será responsável (salvo quando estabeleça um acordo em contrário) pelo tratamento da informação transferida realizado por terciros, que viole os limites ou as normas estabelecidas, a menos que a organização tenha conhecimento ou devesse ter conhecimento de que o terceiro processaria a informação de forma contrária aos princípios e não tome quaisquer medidas razoáveis para evitar ou pôr fim a esse tratamento da informação.

---

[1] Não é necessário aplicar os princípios de aviso ou escolha quando a informação é divulgada a um agente subcontratado para desempenhar tarefas em nome e segundo instruções da organização. Todavia, este tipo de divulgação está sujeito ao princípio de retransferência.

SEGURANÇA

As organizações que criam, mantêm, utilizam ou divulgam ficheiros de informações pessoais devem tomar precauções razoáveis para evitar a perda, utilização indevida e acesso, revelação, alteração ou destruição não autorizados.

INTEGRIDADE DOS DADOS

De acordo com os princípios, as informações pessoais devem ser pertinentes para os fins da sua utilização. Uma organização não pode tratar informações pessoais de modo incompatível com os fins que motivaram a recolha ou que tenham sido autorizados posteriormente pela pessoa em causa. Na medida necessária para se atingirem esses fins, as organizações devem tomar providências razoáveis para assegurar que os dados são fiáveis para a utilização prevista, exactos, completos e actuais.

ACESSO

Os cidadãos devem poder ter acesso às informações pessoais que lhes dizem respeito e que estejam na posse de uma organização; devem poder rectificar, alterar ou eliminar informações inexactas, salvo se os encargos ou as despesas para facultar esse acesso forem desproporcionados em relação aos riscos para a vida privada da pessoa em causa, ou sempre que os legítimos direitos de terceiros incorram em risco de violação.

APLICAÇÃO

A protecção efectiva da vida privada deve incluir mecanismos que garantam o cumprimento dos princípios de «porto seguro», recursos para os cidadãos a que se referem os dados e que tenham sido afectados pelo incumprimento dos princípios, bem como consequências para as organizações sempre que os princípos não sejam seguidos. Estes mecanismos devem incluir, no mínimo: a) mecanismos de recurso independentes, imediatamente disponíveis e pouco onerosos através dos quais as queixas e os litígios dos cidadãos possam ser investigados e resolvidos e os danos reparados sempre que a lei aplicável ou as iniciativas privadas o prevejam, b) procedimentos de acompanhamento para indagar da veracidade das atestações e alegações das empresas em relação às suas práticas em matéria de protecção da vida privada e para verificar se essas práticas relativas à vida privada foram executadas da forma apresentada, e c) a obrigação de solucionar problemas decorrentes do incumprimento dos princípios por organizações que tenham anunciado a sua adesão e consequências para essas organizações. As sanções devem ser suficientemente rigorosas de modo a garantirem o cumprimento por parte das organizações.

Anexo

Lista das entidades públicas nos EUA reconhecidas pela União Europeia

A União Europeia reconhece as seguintes entidades públicas norte-americanas com competência para investigar denúncias, tomar medidas contra práticas desleais e enganosas, assim como proceder à reparação de pessoas singulares, sempre que se verificar incumprimento dos princípios aplicados em conformidade com as orientações das FAQ:

— a Federal Trade Commission com base nas competências que lhe são conferidas pelo artigo 5.º da lei relativa ao comércio federal (Section 5 of the Federal Trade Commission Act),

— o Department of Transportation com base nas competências que lhe são conferidas pelo Title 49 do United States Code, Section 41712.

ANEXO II

QUESTÕES MAIS FREQUENTES (FAQ)

FAQ 1 — Dados sensíveis

Q: *Uma organização deverá sempre propor uma escolha explícita (opção de participação) no que diz respeito aos dados sensíveis?*

R: Não. Esta escolha não é exigida se o tratamento dos dados: 1. se realizar em função de interesses vitais da pessoa em causa ou de outra pessoa, 2. for necessário para a preparação de recursos ou processos judiciais, 3. for necessário para prestar cuidados médicos ou elaborar um diagnóstico, 4. for efectuado no decurso das actividades legítimas de uma fundação, associação ou qualquer outro organismo sem fins lucrativos que possua objectivos políticos, filosóficos, religiosos ou sindicais, na condição de que o tratamento se refira exclusivamente aos membros do organismo ou às pessoas que com ele mantenham contactos habituais no âmbito dos referidos objectivos, e de que os dados não sejam revelados a terceiros sem o consentimento das pessoas em causa, 5. for necessário para que a entidade cumpra as suas obrigações em matéria de direito do trabalho, ou 6. se referir a informação publicada pela pessoa em causa.

FAQ 2 — Excepções jornalísticas

Q: *Tendo em conta a liberdade de imprensa garantida pela Constituição dos EUA, bem como as isenções em matéria de jornalismo previstas pela directiva, os princípios de «porto seguro» aplicam-se às informações de carácter pessoal recolhidas, arquivadas ou divulgadas com fins jornalísticos?*

R: Sempre que o direito de liberdade de imprensa consagrado na Primeira Emenda da Constituição dos EUA não for compatível com os interesses de protecção da vida privada, a Primeira Emenda deverá garantir o equilíbrio de tais interesses no que diz respeito às actividades de pessoas ou de organizações norte-americanas. A informação pessoal recolhida para efeitos de publicação, difusão ou outra forma de comunicação pública de material jornalístico, quer seja, ou não, utilizada, bem como a informação constante de material já publicado e arquivado, não está sujeita aos requisitos dos princípios de «porto seguro».

FAQ 3 — Responsabilidade subsidiária

Q: *Os fornecedores de serviços da internet (ISP), os operadores de telecomunicações ou outras organizações estão sujeitos aos princípios de «porto seguro» quando, em nome de outra organização, se limitam a transmitir, encaminhar, trocar ou guardar informação susceptível de violar estes princípios?*

R: Não. À semelhança da própria directiva, o princípio de «porto seguro» não gera uma responsabilidade subsidiária. Não se poderá responsabilizar uma entidade que aja exclusivamente como transmissora de dados transmitidos por terceiros e não seja determinante nem para a finalidade, nem para os meios de tratamento dos dados pessoais.

FAQ 4 — Bancos de investimento e auditorias

Q: *As actividades de auditores e bancos de investimento podem implicar o tratamento de dados pessoais sem conhecimento do interessado. Quais os casos em que os princípios de aviso, escolha e acesso permitem este tipo de tratamento?*

R: Os bancos de investimento ou os auditores podem tratar informação sem conhecimento do interessado, apenas na medida em que isso se justifique, e pelo tempo necessário, em função de disposições regulamentares ou por razões de interesse público, bem como noutras circunstâncias em que a aplicação desses princípios seja prejudicial aos interesses legítimos das suas organizações. Esses interesses incluem a verificação do cumprimento, por parte das empresas, das suas obrigações legais e actividades contabilísticas legítimas, e a observação da confidencialidade no contexto de possíveis aquisições, fusões, empresas comuns ou transacções semelhantes efectuadas por bancos de investimento ou auditores.

FAQ 5 [1] **— Papel das autoridades responsáveis pela protecção dos dados**

Q: *Que forma adoptarão e como serão aplicados os compromissos de cooperação das empresas com as autoridades europeias responsáveis pela protecção dos dados (APD)?*

R: Em conformidade com os princípios de «porto seguro», as organizações norte-americanas que recebam dados pessoais provenientes da UE devem comprometer-se a utilizar mecanismos eficazes que garantam o cumprimento dos referidos princípios. Concretamente, como definido no princípio de aplicação, devem prever: a) vias de recurso para as pessoas em causa, b) procedimentos de acompanhamento, a fim de verificar a veracidade das afirmações e declarações das organizações em matéria de respeito da vida privada, e c) a obrigação de as referidas organizações solucionarem os problemas que surjam por incumprimento dos princípios, bem como de assumirem as respectivas consequências. Uma organização pode satisfazer as alíneas a) e c) previstas pelo princípio de aplicação, comprometendo-se a cooperar com as APD, nas condições estabelecidas na presente FAQ.

Uma organização pode comprometer-se a cooperar com as autoridades responsáveis pela protecção dos dados declarando na sua certificação de adesão ao «porto seguro» dirigida ao Department of Commerce (ver FAQ 6 — Autocertificação) que:

1. opta por cumprir as alíneas a) e c) do princípio de aplicação do «porto seguro», comprometendo-se a cooperar com as APD,

2. cooperará com as APD na investigação e resolução de queixas formuladas no âmbito do «porto seguro», e

3. respeitará as decisões da APD, sempre que esta considere que a organização deve tomar medidas específicas para cumprir os princípios de «porto seguro», incluindo o pagamento de indemnizações ou compensações às pessoas prejudicadas pelo desrespeito dos princípios, e apresentará à APD confirmação por escrito de que tais medidas foram tomadas.

A cooperação com as APD assumirá as formas de informação e aconselhamento seguintes:

— o aconselhamento das APD será veiculado através de um grupo de trabalho informal composto por estas autoridades à escala europeia, que contribuirá, entre outros aspectos, para assegurar uma abordagem coerente e harmonizada destas questões,

— o mesmo grupo deverá prestar aconselhamento às organizações norte-americanas no que respeita a queixas por resolver apresentadas pelas pessoas cuja informação pessoal, transferida da UE ao abrigo do «porto seguro», tenha sido objecto de tratamento. Esse aconselhamento, que tem por fim garantir a correcta aplicação dos princípios de «porto seguro», contemplará todas as vias de recurso para a(s) pessoa(s) em causa que as APD considerem adequadas,

— o grupo prestará aconselhamento em resposta a queixas trazidas pelas organizações em questão e/ou a queixas apresentadas directamente por particulares contra as organizações que se tenham comprometido a cooperar, para efeitos do cumprimento do «porto seguro», com as APD; estas incentivarão e, se necessário, auxiliarão as pessoas em causa a recorrer, em primeira instância, aos mecanismos internos de resolução de queixas de que as organizações disponham,

— a resposta será emitida após ter sido dada a ambas as partes envolvidas a oportunidade de fornecer todas as informações e provas que considerem necessárias. O grupo procurará responder o mais rapidamente possível, dentro dos limites processuais permitidos, em regra geral nos 60 dias seguintes à recepção da queixa e, se possível, antes de findo esse prazo,

— caso considere adequado, o grupo publicará os resultados da análise das queixas recebidas,

— o aconselhamento facultado em nada responsabiliza o grupo no seu conjunto ou as APD individuais que o compõem.

[1] A inclusão da presente FAQ no conjunto das FAQ depende da aprovação das APD. O texto foi discutido pelas referidas entidades no âmbito do grupo do artigo 29.º, tendo a maioria considerado que era aceitável. Contudo, apenas adoptarão uma posição definitiva no contexto do parecer geral que o grupo irá emitir sobre o conjunto final das FAQ.

Como referido acima, as organizações que optem por esta solução para a resolução de litígios deverão ainda comprometer-se a respeitar as decisões das APD. Se as organizações não aplicarem o conselho da APD num prazo de 25 dias, sem apresentar uma razão válida para o atraso, o grupo comunicará a sua intenção de levar o caso à Federal Trade Commission ou a outro organismo federal ou estadual norte-americano, com competência para tomar medidas de execução em caso de fraude ou prestação de falsas declarações, ou para concluir que o Acordo de Cooperação foi seriamente quebrado devendo, por isso, ser considerado nulo. Nesta última hipótese, o grupo informará o Department of Commerce (ou um seu representante) para que altere a lista de participantes no «porto seguro» em conformidade. Qualquer violação do Acordo de Cooperação com as APD, bem como dos princípios de «porto seguro», será objecto de recurso ao abrigo do artigo 5.º da lei relativa ao comércio federal (Section 5 do Federal Trade Commission Act) ou de outra lei semelhante.

As organizações que escolherem esta opção deverão pagar uma taxa anual destinada aos custos de funcionamento do grupo, podendo ainda ter que pagar quaisquer despesas de tradução necessárias, decorrentes das decisões do grupo sobre as queixas de que são objecto. A taxa anual não excederá 500 dólares dos Estados Unidos (USD), sendo inferior para empresas de menor dimensão.

A opção de cooperar com as APD estará ao dispor das organizações que aderirem ao «porto seguro» durante um período de três anos. Esta solução poderá, contudo, vir a ser reconsiderada pelas APD se o número de organizações norte-americanas que por ela optarem for excessivo.

FAQ 6 — Autocertificação

Q: *De que modo uma organização autocertifica a sua adesão aos princípios de «porto seguro»?*

R: Os benefícios decorrentes da adesão ao «porto seguro» vigoram a partir da data em que cada organização autocertifica junto do Department of Commerce (ou do respectivo representante) a sua adesão aos princípios, em conformidade com as orientações que a seguir se especificam.

Para proceder à autocertificação de adesão aos princípios de «porto seguro», as organizações poderão apresentar ao Department of Commerce (ou a um seu representante) uma carta assinada por um dos responsáveis da organização aderente ao «porto seguro», em nome desta, contendo, no mínimo, a seguinte informação:

1. Designação da organização, endereço postal e de correio electrónico, números de telefone e fax;

2. Descrição das actividades da organização em matéria de informação pessoal recebida da UE; e

3. Descrição da política da organização em matéria de protecção da vida privada no que diz respeito a essa informação pessoal, incluindo: a) o local onde pode ser consultada pelo público, b) a sua data de aplicação, c) o nome do gabinete de contacto para a apresentação de queixas, pedidos de acesso ou quaisquer outros assuntos relacionados com os princípios de «porto seguro», d) os organismos oficiais concretos com competência para deliberar sobre quaisquer queixas contra a organização em matéria de práticas desleais ou desonestas e violações das leis ou normas que regulamentam a protecção da vida privada (e que se encontram referidos no anexo dos princípios), e) a designação de qualquer programa relativo à protecção da vida privada em que a organização participe, f) o método de verificação (por exemplo, interno ou por terceiros) [2], e g) o mecanismo de recurso independente que possa ser utilizado para investigar as queixas por resolver.

Se a organização desejar que a sua adesão aos princípios de «porto seguro» abranja também a informação sobre recursos humanos transferida da UE para ser utilizada num contexto de relações laborais pode fazê-lo, desde que exista um organismo oficial com competência para conhecer de queixas contra a referida organização, em matéria de informações sobre recursos humanos, referido na lista anexa aos princípios. Além disso, deve declarar na sua autocertificação que deseja abranger esse tipo de informações, que deseja colaborar com as autoridades da UE, em conformidade com as FAQ 9 e 5, consoante o caso, e que acatará o parecer emitido por essas autoridades.

O Department of Commerce (ou o seu representante) terá uma lista de todas as organizações que autocertificarem a sua adesão ao «porto seguro», garantindo desta forma os benefícios daí decorrentes, que actualizará com base nas cartas anuais e notificações que receba, de acordo com a FAQ 11. Estas cartas de autocertificação deverão ser apresentadas, no mínimo, uma vez por ano, caso contrário as organizações serão suprimidas da lista e deixarão de usu-

[2] Ver FAQ 7 — Verificação.

fruir dos benefícios decorrentes do «porto seguro». Tanto a lista como as cartas de autocertificação enviadas pelas organizações serão colocadas à disposição do público. Todas as organizações que autocertificarem a sua adesão aos princípios de «porto seguro» deverão também mencionar nas respectivas declarações públicas relativas à sua política em matéria de protecção da vida privada que aderem aos princípios de «porto seguro».

O compromisso de adesão aos princípios de «porto seguro» não se limita apenas aos dados recebidos durante o período em que a organização usufrui dos benefícios daí decorrentes, já que, ao aderir, a organização se compromete a aplicar os ditos princípios aos dados em questão enquanto os armazenar, utilizar ou revelar, mesmo que, posteriormente, decida por qualquer motivo abandonar o «porto seguro».

Uma organização que cesse como entidade jurídica separada, ne sequência de uma fusão ou de uma aquisição, deve antecipadamente informar desse facto o Department of Commerce ou o seu representante. A notificação deve ainda indicar se a nova entidade resultante da fusão ou da aquisição: 1. continuará abrangida pelo «porto seguro» por força do instrumento legal que regulou a fusão ou aquisição, ou 2. decide autocertificar a sua adesão aos princípios ou aplicar outro tipo de garantias, como um acordo escrito que garanta a adesão aos princípios. Quando nenhuma destas duas condições se aplicar, quaisquer dados que tenham sido recebidos no âmbito do «porto seguro» devem ser prontamente cancelados.

Se bem que uma organização não tenha de subordinar todas as informações pessoais ao «porto seguro», a partir do momento da sua adesão aos princípios todos os dados pessoais que receba da UE deverão ser abrangidos por eles.

Qualquer declaração falsa prestada ao público relativa à adesão aos princípios de «porto seguro» poderá ser objecto de recurso junto da Federal Trade Commission ou de qualquer outra instância governamental competente. As declarações falsas prestadas ao Department of Commerce (ou a um seu representante) poderão ser objecto de recurso ao abrigo da legislação sobre falsos testemunhos (False Statements Act — 18 USC § 1001).

FAQ 7 — Verificação

Q: *Como é que as organizações prevêem modalidades de acompanhamento para verificar não só se os certificados e as declarações das empresas sobre as suas práticas em matéria de privacidade, no âmbito do «porto seguro», correspondem à verdade, como também se essas práticas em matéria de privacidade foram aplicadas em conformidade com as declarações prestadas e com os princípios de «porto seguro»?*

R: Para cumprir os requisitos de verificação do princípio de aplicação, uma organização pode verificar os certificados e as declarações recorrendo quer a uma auto-avaliação quer a verificações de conformidade externas.

No caso da auto-avaliação, esta verificação deve indicar se a política pública da organização em matéria de protecção da vida privada no que respeita à informação pessoal recebida da UE é exacta, abrangente, claramente exposta, completamente aplicada e acessível. Deverá, também, indicar que a sua política em matéria de protecção da vida privada está conforme aos princípios de «porto seguro», que as pessoas estão informadas sobre os instrumentos internos específicos de que a organização dispõe para processar as queixas e sobre os mecanismos independentes de apresentação de queixas, que a organização instituiu procedimentos específicos, que os trabalhadores receberam formação adequada para a sua aplicação e que se aplicam sanções em caso de não cumprimento dos mesmos e, por fim, que estão em vigor procedimentos internos para a realização periódica de verificações de conformidade com o acima exposto. A declaração de verificação da auto-avaliação, que deverá ser assinada por um responsável da empresa, ou por qualquer outro representante autorizado, deve ser efectuada, no mínimo, uma vez por ano e posta à disposição das pessoas, mediante pedido ou no âmbito de uma investigação ou de queixa por motivos de não conformidade.

As organizações devem manter registos relativos à aplicação das suas práticas em matéria de privacidade no âmbito do «porto seguro», que devem ser postos à disposição, mediante pedido, no âmbito de uma investigação ou queixa relativa à conformidade, da entidade independente responsável pela investigação da queixa ou da agência responsável em matéria de práticas desleais e desonestas.

Se a organização tiver optado por verificações de conformidade externas, essas verificações deverão atestar que a sua política em matéria de protecção da vida privada no que respeita à informação pessoal recebida da UE é conforme aos princípios de «porto seguro» e está a ser devidamente cumprida, e que as pessoas são informadas dos mecanismos ao seu dispor para apresentar queixa. Os métodos de verificação poderão compreender, consoante os casos, auditorias sem restrições, verificações aleatórias, o recurso a simulações ou o uso de instrumentos tecnológicos. A declaração atestando a realização da verificação de conformidade externa, que deverá ser assinada pelo res-

ponsável da verificação ou pelo responsável da empresa ou um outro representante autorizado, deve ser efectuada, no mínimo, uma vez por ano, e posta à disposição das pessoas, mediante pedido ou no âmbito de uma investigação ou queixa relativa à conformidade.

FAQ 8 — Acesso

Princípio de acesso

As pessoas devem ter acesso às informações pessoais na posse de uma organização e poder corrigir, alterar ou suprimir as mesmas, sempre que forem incorrectas, excepto nos casos em que a autorização de acesso comporte encargos desproporcionados em relação aos riscos para a vida privada da pessoa em causa, ou em situações que impliquem a violação dos direitos legítimos de terceiros.

Q 1: *O direito de acesso é absoluto?*

R 1: Não. No âmbito dos princípios de «porto seguro», o direito de acesso é fundamental para a protecção da vida privada. Permite, em especial, que as pessoas verifiquem a exactidão das informações que outras entidades possuem a seu respeito. Em qualquer caso, a obrigação, por parte da organização detentora da informação, de garantir acesso à mesma está sujeita ao princípio da proporcionalidade ou da razoabilidade e, em certas ocasiões, deve ser moderada. Com efeito, a exposição de motivos das directrizes da OCDE em matéria de protecção da vida privada, publicadas em 1980, indica claramente que a obrigação de acesso que incumbe a uma organização não é absoluta. Não exige, por exemplo, as investigações extremamente meticulosas que são necessárias no caso de uma citação, nem sequer implica o acesso às diversas formas sob as quais a organização detenha as referidas informações.

Pelo conrário, a experiência mostra que, ao satisfazer os pedidos de acesso por parte das pessoas, as organizações devem guiar-se, em primeiro lugar, pelas preocupações que deram lugar ao pedido. Por exemplo, se um pedido de acesso é vago ou muito geral, a organização poderá entrar em diálogo com o interessado, a fim de tentar compreender qual a motivação subjacente ao pedido e poder prestar as informações adequadas. A organização pode desejar saber qual, ou quais, dos seus serviços a pessoa contactou e/ou a natureza da informação (ou a sua utilização) que é objecto do pedido de acesso. As pessoas não são, todavia, obrigadas a justificar um pedido de acesso aos seus próprios dados.

As despesas e os encargos são factores importantes a ter em conta, embora não sejam determinantes para avaliar a razoabilidade de um pedido de acesso. Se a informação é utilizada para tomar decisões que poderão afectar significativamente a pessoa em questão (por exemplo, a recusa ou concessão de benefícios consideráveis como seguros, hipotecas ou um emprego), a organização terá, em conformidade com as restantes disposições destas FAQ, de divulgar a referida informação, mesmo que isso se revele relativamente difícil ou dispendioso.

Se as informações solicitadas não forem de carácter sensível, nem forem utilizadas para tomar decisões que afectem consideravelmente a pessoa (por exemplo, dados de *marketing* sem carácter sensível, utilizados para determinar o envio ou não de um catálogo a uma pessoa), mas a sua disponibilização for fácil e pouco dispendiosa, a organização deve facultar o acesso às informações concretas que possui, relativas à pessoa que efectuou o pedido. A informação em causa poderá incluir dados fornecidos pela própria pessoa, dados recolhidos no decurso de uma transacção ou dados que digam respeito à pessoa, obtidos através de terceiros.

Uma vez que o princípio de acesso é fundamental, as organizações devem sempre, de boa fé, envidar todos os esforços para conceder o acesso. Nos casos em que determinada informação exija protecção e se distinga com facilidade de outra informação que seja objecto de um pedido de acesso, a organização deverá reter a informação protegida e disponibilizar os restantes dados. Se uma organização decidir recusar o acesso em qualquer circunstância, deverá prestar à pessoa que o solicitou a devida justificação e informação sobre os contactos a efectuar para posteriores investigações.

Q 2: *O que se entende por informações comerciais confidenciais? A sua salvaguarda justifica que as organizações neguem o acesso a esse tipo de informações?*

R 2: As informações comerciais confidenciais (na acepção das Federal Rules of Civil Procedures on discovery, no âmbito da divulgação de informação) são dados relativamente aos quais uma organização toma medidas de protecção para que não sejam divulgados, sempre que possam ser utilizados para beneficiar a concorrência. O programa informático específico utilizado pela organização, como, por exemplo, um programa de elaboração de modelos ou os detalhes deste programa, podem constituir informações comerciais confidenciais. Nos casos em

que a informação se distinga com facilidade de outra informação que seja objecto de um pedido de acesso, a organização deverá reter a informação comercial confidencial e disponibilizar a que não é confidencial. As organizações podem recusar ou limitar o acesso na medida em que este implique revelar informações comerciais confidenciais a seu respeito, tal como acima definidas, como é o caso das deduções ou classificações de *marketing* produzidas pela organização, ou informações comerciais confidenciais de terceiros, nos casos em que estas informações sejam objecto de uma obrigação contratual de confidencialidade, em circunstâncias em que tal obrigação deveria, normalmente, ser aceite ou imposta.

Q 3: *Quando garante o acesso, uma organização pode limitar-se a comunicar às pessoas os dados pessoais que lhes dizem respeito arquivados nas suas bases de dados ou deve garantir o acesso à própria base de dados?*

R 3: O acesso pode ser garantido sob a forma de prestação de informações ao requerente, sem que haja necessidade de lhe conceder o acesso à base de dados da organização.

Q 4: *Uma organização deve reestruturar as suas bases de dados a fim de poder garantir o acesso às mesmas?*

R 4: O acesso apenas tem de ser concedido na medida em que a organização armazene a informação. O princípio de acesso não deve, por si, criar qualquer obrigação de recolha, manutenção, reorganização ou reestruturação de ficheiros de informações pessoais.

Q 5: *Estas respostas ilustram claramente que o acesso pode ser recusado em determinadas circunstâncias. Quais as restantes circunstâncias em que as organizações podem recusar o acesso das pessoas às informações que lhes dizem respeito?*

R 5: O acesso apenas pode ser recusado em circunstâncias limitadas e quaisquer razões apresentadas para justificar a recusa devem ser específicas. Uma organização pode recusar-se a dar acesso a informações, sempre que a divulgação seja passível de interferir com a salvaguarda de interesses públicos igualmente importantes, nomeadamente a segurança nacional, defesa ou segurança pública. Além disso, o acesso pode ser recusado quando a informação pessoal é tratada *apenas* para fins estatísticos ou de investigação. Outras razões para recusar ou limitar o acesso:

a) Interferência com a execução ou o cumprimento da lei, incluindo a prevenção, investigação ou detecção de delitos ou o direito a um processo equitativo;

b) Interferência com processos particulares, incluindo a prevenção, investigação ou detecção de queixas ou o direito a um processo equitativo;

c) Divulgação de informação pessoal que contenha referências a outra(s) pessoa(s), nos casos em que estas referências não possam ser separadas;

d) Quebra de uma obrigação ou privilégio de carácter jurídico ou profissional;

e) Quebra da indispensável confidencialidade das negociações em curso ou a realizar no futuro, por exemplo, as relacionadas com a aquisição de empresas cotadas na bolsa;

f) Prejuízo de investigações no âmbito da segurança dos trabalhadores ou de procedimentos de resolução de queixas;

g) Prejuízo da confidencialidade que poderá ser necessária, durante períodos limitados, para a planificação da sucessão dos trabalhadores e as reorganizações das empresas; ou

h) Prejuízo da confidencialidade que poderá ser necessária em matéria de acompanhamento, inspecções ou funções de regulamentação relativas a uma boa gestão económica ou financeira; ou

i) Outras circunstâncias em que o acesso signifique encargos ou custos desproporcionados ou represente violação dos direitos legítimos ou interesses de terceiros.

Cabe à organização que invocar a excepção demonstrar o seu fundamento (como habitualmente acontece). Tal como acima se refere, as razões de recusa ou restrição do acesso, bem como um ponto de contacto para a obtenção de mais esclarecimentos devem ser indicados às pessoas que o solicitem.

Q 6: *Uma organização pode cobrar uma taxa a fim de cobrir os encargos de acesso?*

R 6: Sim. As directrizes da OCDE reconhecem que as organizações poderão cobrar uma taxa, desde que não seja excessiva. As organizações podem, assim, solicitar o pagamento de uma taxa razoável para garantir o acesso à informação. A cobrança de uma taxa poderá ser útil para desencorajar pedidos repetidos ou abusivos.

As organizações especializadas na venda de informações acessíveis ao público podem, assim, responder ao pedido de acesso contra pagamento de uma taxa correspondente ao montante habitualmente cobrado pela organização. Alternativamente, as pessoas podem procurar obter a sua informação na primeira organização que originalmente reuniu os dados.

O acesso não pode ser recusado por razões relacionadas com os custos se a pessoa em causa se propuser pagá-los.

Q 7: *Uma organização é obrigada a garantir o acesso a informações pessoais obtidas a partir de registos públicos?*

R 7: Em primeiro lugar, convém esclarecer que os registos públicos são todos os arquivos conservados pelos organismos ou entidades estatais, a todos os níveis, que podem ser consultados pelo público em geral. A aplicação dos princípios de acesso às informações não é necessária desde que estas não estejam associadas a outras informações pessoais, excepto nos casos em que uma quantidade mínima de informações que não fazem parte dos registos públicos é utilizada para catalogar ou organizar a informação desses registos. Contudo, devem respeitar-se as condições de consulta exigidas pela respectiva instância de jurisdição. Quando as informações dos registos públicos estão associadas a informações não provenientes de outros registos públicos, uma organização deve garantir o acesso a toda a informação, partindo do princípio de que esta não é objecto de outras excepções autorizadas.

Q 8: *O princípio de acesso deve ser aplicado a toda a informação pessoal disponível ao público?*

R 8: À semelhança das informações obtidas a partir de registos públicos (ver Q 7), não é necessário aplicar o princípio de acesso a informação que já seja disponibilizada ao grande público, desde que não esteja associada a informação não pública.

Q 9: *Como é que uma organização se pode proteger contra pedidos de acesso repetidos ou abusivos?*

R 9: Uma organização não é obrigada a satisfazer esses pedidos de acesso. Por esse motivo, as organizações podem solicitar o pagamento de uma taxa razoável e poderão determinar limites razoáveis relativos ao número de vezes que, durante um dado período, se dará resposta aos pedidos de uma determinada pessoa. Ao definir estas limitações, uma organização deverá considerar determinados factores, como, por exemplo, a frequência das actualizações da informação, a finalidade da utilização dos dados e a natureza da informação.

Q 10: *Como é que uma organização se pode proteger contra pedidos de acesso fraudulentos?*

R 10: Uma organização não é obrigada a garantir o acesso à informação se não lhe forem fornecidos dados suficientes que lhe permitam confirmar a identidade da pessoa que efectua o pedido.

Q 11: *Existe algum prazo para responder aos pedidos de acesso?*

R 11: Sim. As organizações devem dar resposta aos pedidos sem atrasos excessivos e dentro de um prazo razoável. Este requisito poderá ser preenchido de diversas formas, tal como se especifica na exposição de motivos das directrizes da OCDE em matéria de protecção da vida privada, publicadas em 1980. Por exemplo, um responsável pelo tratamento dos dados que fornece, regularmente, informações às pessoas que são objecto das mesmas poderá ficar isento da obrigação de responder imediatamente a um pedido individual.

FAQ 9 — Recursos humanos

Q 1: *A transferência da UE para os Estados Unidos de dados pessoais recolhidos no âmbito de relações de trabalho é abrangida pelos princípios de «porto seguro»?*

R 1: Sim. Quando uma empresa da UE transfere dados pessoais relativos aos seus trabalhadores (anteriores ou actuais), recolhidos no âmbito da relação de trabalho, para uma empresa-mãe, uma entidade associada ou um fornecedor de serviços não associado nos Estados Unidos que tenha aderido aos princípios de «porto seguro», a transferência

goza das condições garantidas pelos princípios. Nestes casos, a recolha de informação e o seu tratamento antes de efectuada a transferência deverão estar sujeitos à legislação nacional do país da UE onde se processou a recolha, bem como às condições ou restrições impostas à transferência que serão respeitadas de acordo com essa mesma legislação.

Os princípios de «porto seguro» são pertinentes apenas no caso da transferência ou do acesso a registos individualmente identificados. As estatísticas baseadas em dados agregados sobre o emprego e/ou o uso de dados anónimos ou apresentados sob pseudónimo não levantam quaisquer preocupações em matéria de privacidade.

Q 2: *Como se aplicam os princípios de aviso e de escolha aos dados em questão?*

R 2: Uma organização norte-americana que receba informações abrangidas pelo «porto seguro», provenientes da UE, relativas a trabalhadores, só poderá divulgá-las a terceiros e/ou utilizá-las de forma diversa dos objectivos que presidiram à recolha inicial, em conformidade com os princípios de aviso e de escolha. Por exemplo, se uma organização pretender utilizar informações pessoais inicialmente recolhidas no âmbito de relações de trabalho para fins alheios à relação de trabalho, tais como, para fins de comunicações de *marketing*, a organização norte-americana deve, antes de mais, garantir às pessoas em causa o direito de escolha, a não ser que estas tenham já autorizado o uso da informação para tais fins. Além disso, qualquer escolha efectuada pelo trabalhador não poderá ser utilizada para limitar as oportunidades de emprego ou aplicar sanções ao referido trabalhador.

Note-se que certas condições gerais aplicáveis às transferências a partir de determinados Estados-Membros podem excluir o uso da informação para diferentes finalidades, mesmo após efectuada a sua transferência para fora da UE; nesses casos, as referidas condições terão que ser respeitadas.

Acrescente-se que os empregadores devem envidar esforços consideráveis no sentido de respeitar as opções dos trabalhadores em matéria de privacidade, podendo, por exemplo, limitar o acesso aos dados, garantir o anonimato em relação a certos dados ou a atribuição de pseudónimos sempre que os nomes reais não sejam necessários para o objectivo de gestão em causa.

A organização não aplicará os princípios de aviso e de escolha, na medida e durante o tempo que assim se justifique para não prejudicar os interesses legítimos da organização em matéria de promoções, nomeações ou outras decisões de índole semelhante.

Q 3: *Como se aplica o princípio de acesso?*

R 3: As FAQ relativas ao acesso fornecem orientações sobre os motivos que podem justificar, recusar ou limitar o acesso solicitado no contexto dos recursos humanos. É evidente que os empregadores comunitários devem agir em conformidade com os regulamentos locais e assegurar que os trabalhadores comunitários tenham acesso à informação nos moldes exigidos pela legislação dos seus países de origem, independentemente do local onde se tratam ou arquivam os dados. Os princípios de «porto seguro» exigem a colaboração da organização responsável pelo tratamento destes dados nos Estados Unidos, a qual deverá garantir o acesso, quer directamente, quer através do empregador comunitário.

Q 4: *Como será controlado o respeito pelos dados relativos aos trabalhadores no âmbito dos princípios de «porto seguro»?*

R 4: Quando a informação for exclusivamente utilizada no âmbito das relações de trabalho, a empresa na UE será a principal responsável pelos dados perante o trabalhador. Por esse motivo, sempre que os trabalhadores europeus apresentem uma queixa relativa à violação dos seus direitos em matéria de protecção dos dados e não estiverem satisfeitos com os resultados dos processos de verificação interna, reclamação e recurso (ou com qualquer outro procedimento de resolução de queixas no âmbito de um contrato com um sindicato), deverão ser aconselhados a dirigir-se às entidades nacionais responsáveis pela protecção dos dados ou à autoridade laboral da jurisdição onde trabalham. Também se incluem aqui os casos em que a alegada utilização incorrecta dos seus dados pessoais tenha ocorrido nos Estados Unidos, seja da responsabilidade da organização norte-americana que recebeu os dados fornecidos pelo empregador e não responsabilidade deste, e implique, por conseguinte, uma alegada violação dos princípios de «porto seguro», e não da legislação nacional de transposição da directiva. Esta será a forma mais eficaz de abordar os direitos e obrigações, que muitas vezes se sobrepõem, impostos pelas convenções, pela legislação local do trabalho e pela legislação relativa à protecção dos dados.

Uma organização norte-americana aderente ao «porto seguro» que utilize os dados relativos aos recursos humanos comunitários transferidos da União Europeia, no âmbito das relações de trabalho, e que pretenda que tais transferências de dados sejam abrangidas pelos princípios de «porto seguro» tem, por conseguinte, de se comprometer a colaborar em qualquer investigação e a agir em conformidade com as orientações das autoridades comunitárias competentes na matéria. As APD que tenham decidido cooperar deste modo notificarão do facto a Comissão

Europeia e o Department of Commerce. Se uma organização norte-americana aderente ao «porto seguro» pretender transferir dados relativos a recursos humanos a partir de um Estado-Membro cuja APD não tenha tomado tal decisão, aplica-se o disposto na FAQ 5 ([3]).

FAQ 10 — Contratos «artigo 17.º»

Q: *Quando os dados são transferidos da UE para os EUA com o objectivo exclusivo do seu tratamento (subcontratação), será necessário um contrato apesar da participação do responsável pelo tratamento no «porto seguro»?*

R: Sim. Na Europa, os responsáveis pelo tratamento de dados são obrigados a celebrar contrato quando se efectua uma transferência para tratamento (subcontratação), seja esta processada no interior ou no exterior da UE. O objectivo do contrato é proteger os interesses do responsável pelo tratamento de dados, isto é, a pessoa ou a organização que determina os objectivos e os meios do tratamento e é totalmente responsável pelos dados relativamente à(s) pessoa(s) em questão. O contrato especifica, assim, o tratamento a efectuar e quaisquer outras medidas necessárias para garantir a segurança desses mesmos dados.

As organizações dos EUA aderentes ao «porto seguro» que recebam informação de carácter pessoal da UE para mero tratamento não têm, assim, que aplicar os princípios a esta informação, visto que o responsável pelo tratamento de dados na UE permanece responsável perante a pessoa, de acordo com as disposições da legislação comunitária (que podem ser mais rigorosas do que os próprios princípios de «porto seguro»).

Visto que os princípios de «porto seguro» garantem protecção adequada, os contratos com os participantes celebrados para mero tratamento não exigem autorização prévia (ou essa autorização será automaticamente garantida pelos Estados-Membros), contrariamente aos contratos com destinatários que não tenham aderido aos referidos princípios ou que não apliquem outra modalidade de protecção adequada.

FAQ 11 — Resolução de litígios e aplicação

Q: *Como deverão ser implementados os requisitos de resolução de litígios previstos no princípio de aplicação e como deverá ser tratado o problema de uma organização que persista em não cumprir os princípios?*

R: O princípio de aplicação estabelece os requisitos observados pelos mecanismos de aplicação dos princípios de «porto seguro». Como cumprir os requistitos do ponto b) do princípio consta da FAQ sobre verificação (FAQ 7). A presente FAQ (FAQ 11) aborda os pontos a) e c) que exigem mecanismos de recurso independentes. Esses mecanismos podem assumir formas diferentes, mas todos devem cumprir os requisitos do princípio de aplicação. As organizações podem cumprir os requisitos das seguintes maneiras: 1. aplicando programas do sector privado de protecção da privacidade que respeitem os princípios de «porto seguro» nas suas regras e que incluam mecanismos de aplicação efectivamente eficazes do tipo descrito no princípio de aplicação, 2. obedecendo às regras estabelecidas por entidades de controlo legal ou regulamentar que prevejam o tratamento de queixas individuais e resolução de litígios, ou 3. comprometendo-se a cooperar com as autoridades de protecção dos dados da Comunidade Europeia ou os seus representantes autorizados. Esta lista pretende ser ilustrativa sem ser limitativa. O sector privado pode criar outros mecanismos de aplicação, desde que os mesmos cumpram o estabelecido no princípio de aplicação e nas FAQ. É de referir que os requisitos do princípio de aplicação complementam o requisito, estabelecido no n.º 3 da introdução aos princípios, segundo o qual as iniciativas de auto-regulamentação devem ser vinculativas, em conformidade com o artigo 5.º da lei relativa ao comércio federal (Federal Trade Commission Act) ou regulamentação semelhante.

Mecanismos de recurso

Antes de mais, as pessoas devem ser encorajadas a apresentar queixas que possam ter à organização em causa, antes de recorrerem a mecanismos de recurso independentes. A independência de um mecanismo de recurso é um dado factual e pode ser demonstrado de várias maneiras diferentes, por exemplo, através da transparência da composição e do financiamento ou de antecedentes meritórios comprovados. Como exigido pelo princípio de aplicação,

([3]) As disposições da FAQ 5 referem um período de vigência de três anos. O grupo do artigo 29.º deverá analisar o modo de garantir uma solução permanente para os dados relativos aos trabalhadores.

o recurso colocado à disposição das pessoas deve ser de fácil utilização e pouco oneroso. Os organismos para resolução de litígios devem investigar cada uma das queixas apresentadas pelas pessoas, a menos que se trate de queixas infundadas ou abusivas, o que não impedirá que a organização que gere o mecanismo de recurso estabeleça requisitos de elegibilidade; todavia, tais requisitos deverão ser transparentes e justificados (por exemplo, para excluir queixas que não se inserem no âmbito do programa ou que devam ser analisadas noutras instâncias), sem pôr em causa o compromisso de analisar queixas legítimas. Ademais, os mecanismos de recurso devem facultar às pessoas, no momento em que apresentam a respectiva queixa, informação completa e prontamente disponível sobre o funcionamento do mecanismo de resolução de litígios. A informação deverá incluir indicações sobre as práticas desse mecanismo em matéria de privacidade, em conformidade com os princípios de «porto seguro» ([4]). Deverão também cooperar no desenvolvimento de novos instrumentos, como formulários-tipo para apresentação de queixa, que facilitem o procedimento de resolução de litígios.

Reparação e sanções

O resultado de quaisquer reparações decididas pelo organismo para resolução de litígios deve ser de molde a garantir que os efeitos do incumprimento sejam anulados ou corrigidos pela organização, na medida do possível, e que, no futuro, a organização proceda em conformidade com os princípios, podendo mesmo, se tal for oportuno, deixar de processar os dados da pessoa que apresentou queixa. As sanções devem ser suficientemente rigorosas para garantir que a organização se conforme aos princípios. Um conjunto de sanções de diferentes graus de severidade permitirá que os organismos para resolução de litígios reajam adequadamente aos vários níveis de incumprimento. As sanções devem incluir tanto a publicação de casos de incumprimento como a supressão de dados, em determinadas circunstâncias ([5]). Outras sanções podem consistir na suspensão ou retirada de autorização, em compensações a pessoas que sofram perdas decorrentes de não conformidade e injunções. Os organismos de auto-regulamentação e para resolução de litígios do sector privado têm que informar, se for caso disso, os tribunais ou as entidades governamentais com competência na matéria, sempre que tenham conhecimento de violação das regras por parte das organizações aderentes ao «porto seguro», bem como o Department of Commerce, ou um seu representante.

Actividade da FTC

A FTC (Federal Trade Commission) comprometeu-se a examinar prioritariamente as queixas trazidas por organizações privadas de auto-regulamentação, como BBBOnline e TRUSTe, e as dos Estados-Membros da UE em matéria de incumprimento dos princípios de «porto seguro», para determinar se há violação do artigo 5.º da lei relativa à Comissão reguladora do comércio federal (Section 5 of the Federal Trade Commission Act), que proíbe os actos ou as práticas desleais ou enganosas. Se a FTC concluir que tem razão(ões) para considerar que o artigo 5.º foi violado, pode resolver o assunto procurando obter uma decisão administrativa para fazer cessar e proibir as práticas denunciadas ou através de apresentação de uma queixa a um tribunal federal distrital, que se tiver êxito pode resultar numa decisão do tribunal com o mesmo efeito. A FTC pode obter sanções de carácter civil por violação de uma decisão desse tipo e pode intentar uma acção cível ou penal por violação de uma decisão do tribunal federal. A FTC informará o Department of Commerce de qualquer acção que empreender. O Department of Commerce encoraja outros organismos governamentais a informá-lo sobre as decisões judiciais deste tipo ou sobre quaisquer outras disposições relativas à adesão aos princípios de «porto seguro».

Incumprimento persistente

Caso determinada organização persista em não cumprir os princípios, deixará de beneficiar do «porto seguro». O incumprimento permanente ocorre sempre que uma organização que tenha apresentado ao Department of Commerce (ou um seu representante) a respectiva autocertificação recuse cumprir a decisão final de um organismo de auto-regulamentação ou estatal, ou que um desses organismos constate que uma organização desrespeita frequentemente os princípios, a ponto de o seu empenho no cumprimento dos princípios deixar de ser credível. Nestes casos, a organização deve informar imediatamente o Department of Commerce (ou um seu representante) desse facto. Se não o fizer sujeitar-se-á a processo judicial ao abrigo da legislação sobre falsos testemunhos (False Statements Act).

O Department of Commerce (ou um seu representante) indicará na lista que mantém sobre as organizações que aderiram aos princípios de «porto seguro» todas as informações relativas a incumprimento persistente, quer provenham da própria organização, de um organismo de auto-regulamentação ou de um organismo governamental; contudo, só poderá fazê-lo após ter dado um prazo de trinta (30) dias e uma oportunidade de resposta à organização em falta. De igual modo, a lista pública do Department of Commerce (ou um seu representante) indicará claramente quais as organizações que beneficiam do «porto seguro» e as que dele deixaram de beneficiar.

([4]) Os organismos para resolução de litígios não são obrigados a serem conformes com o princípio de aplicação, podendo igualmente derrogar aos princípios quando se depararem com obrigações contraditórias ou autorizações explícitas no desempenho das suas tarefas específicas.

([5]) Os organsimsos para resolução de litígios têm poder discricionário no que se refere às circunstâncias em que aplicam estas sanções. Um dos factores a considerar quando se toma a decisão de suprimir ou não os dados é o carácter sensível dos mesmos; deverá tomar-se também em consideração se a organização recolheu, utilizou ou divulgou informações em infracção flagrante aos princípios.

Uma organização que pretenda participar num organismo de auto-regulamentação, com o objectivo de voltar a aderir aos princípios de «porto seguro», deverá facultar a esse organismo todas as informações referentes à sua participação anterior nos referidos princípios.

FAQ 12 — Prazo da opção de não participação

Q: *O princípio de escolha permite que uma pessoa exerça a opção apenas no início da relação contratual ou em qualquer altura?*

R: Em geral, o objectivo do princípio de escolha é o de assegurar que as informações pessoais sejam utilizadas e divulgadas de uma forma compatível com as expectativas e opções da pessoa em causa. Por conseguinte, uma pessoa deve poder exercer em qualquer altura a opção de não participação, no que diz respeito à utilização de informações pessoais para fins de *marketing* directo, respeitando, contudo, quaisquer prazos razoáveis estabelecidos pela organização, para que esta disponha de tempo para aplicar a dita opção. Uma organização poderá também exigir informação suficiente que confirme a identidade da pessoa que solicita a não participação. Nos Estados Unidos, as pessoas podem exercer esta opção através de um programa central de não participação, como, por exemplo, o serviço de preferências no envio de publicidade pelo correio da associação de *marketing* directo (Direct Marketing Association's Mail Preference Service). As organizações que recorram a este serviço devem fomentar a respectiva utilização junto dos consumidores que não desejem receber informações comerciais. Em todo o caso, as pessoas deverão poder recorrer a mecanismos imediatamente disponíveis e pouco onerosos que lhes permitam o exercício desta opção.

Do mesmo modo, uma organização poderá utilizar informações para determinados fins de *marketing* directo, nos casos em que é impraticável dar à pessoa a oportunidade de optar pela não participação antes de utilizar a dita informação, desde que, imediatamente a seguir (ou em qualquer outra altura, mediante pedido), a organização garanta à pessoa a opção de recusar (sem qualquer encargo para ela) a recepção de qualquer outra correspondência de *marketing* directo e actue em conformidade com os desejos dessa pessoa.

FAQ 13 — Informação relacionada com viagens

Q: *Em que ocasiões se pode transferir para organizações no exterior da UE a informação proveniente das reservas de bilhetes de avião e outras, relacionadas com viagens, por exemplo, a relativa a passageiros frequentes, a reservas em hotéis e necessidades especiais, como regimes alimentares impostos por razões religiosas ou assistência médica?*

R: Esse tipo de informação pode ser transferida em várias circunstâncias diferentes. De acordo com o artigo 26.º da directiva, a transferência de dados pessoais «para um país terceiro que não assegure um nível de protecção adequado na acepção do n.º 2 do artigo 25.º» poderá ter lugar desde que: 1. seja necessária para o fornecimento de serviços exigidos pelas pessoas, ou para a execução do acordo de «passageiro frequente», por exemplo, ou 2. a pessoa em causa tenha dado de forma inequívoca o seu consentimento à transferência. As organizações norte-americanas aderentes aos princípios de «porto seguro» asseguram uma protecção adequada dos dados pessoais, pelo que podem receber transferências de dados da UE, mesmo que não respeitem essas ou outras condições estabelecidas no artigo 26.º da directiva. Dado que o «porto seguro» contém normas específicas em matéria de informações sensíveis, esse tipo de informação (que, por exemplo, poderá ter de ser obtido em virtude da necessidade de assistência médica da pessoa) poderá incluir-se nas transferências para as organizações aderentes. Em todo o caso, a organização que procede à transferência deve respeitar a legislação do Estado-Membro da UE onde se encontra, o qual poderá, nomeadamente, impor condições especiais de tratamento de dados sensíveis.

FAQ 14 — Produtos farmacêuticos e medicinais

Q 1: *Se os dados pessoais forem recolhidos na União Europeia e transferidos para os EUA para investigação farmacêutica e/ou outros fins, as leis dos Estados-Membros ou os princípios de «porto seguro» são aplicáveis?*

R 1: As leis dos Estados-Membros aplicam-se à recolha de dados pessoais e a qualquer tratamento que tenha lugar antes da transferência para os EUA. Os princípios de «porto seguro» aplicam-se aos dados após a tranferência para os EUA. Os dados utilizados para investigação farmacêutica e outros fins deveriam, se possível, ser anónimos.

Q 2: *Os dados pessoais apurados em estudos de investigação médicos ou farmacêuticos específicos desempenham frequentemente um papel importante na investigação científica futura. Nos casos em que os dados pessoais recolhidos no âmbito de um estudo de investigação são transferidos para uma organização dos EUA aderente ao «porto seguro», pode a mesma utilizá-los para uma nova actividade de investigação científica?*

R 2: Sim, se os princípios de aviso e escolha tiverem sido apropriadamente respeitados desde o início. O aviso deve conter informação sobre quaisquer futuras utilizações específicas dos dados, como seguimentos periódicos, estudos conexos ou *marketing*. É compreensível que nem todas as utilizações futuras dos dados possam ser especificadas, dado que uma nova utilização para fins de investigação pode surgir de análises posteriores dos dados originais, de novas descobertas e progressos médicos, e de desenvolvimentos em matéria de regulamentação e de saúde pública. Se necessário, o aviso deve, por conseguinte, indicar que os dados pessoais podem futuramente ser utilizados em actividades não previstas de investigação médica e farmacêutica. Se essa utilização não for coerente com o(s) objectivo(s) geral(is) da investigação para a qual os dados foram originalmente recolhidos, ou à qual o indivíduo deu posteriormente o seu consentimento, deverá ser obtido um novo consentimento.

Q 3: *O que acontece aos dados relativos a um participante se este decidir, voluntariamente ou a pedido do patrocinador, retirar-se do ensaio clínico?*

R 3: Os participantes podem a todo momento decidir retirar-se de um ensaio clínico, ou ser solicitados a fazê-lo. Quaisquer dados recolhidos antes da retirada podem ainda ser tratados juntamente com outros dados recolhidos no âmbito do ensaio clínico a condição que isso tenha sido esclarecido no aviso comunicado ao participante no momento em que o mesmo concordou participar.

Q 4: *É permitido às empresas de dispositivos farmacêuticos e médicos fornecer dados pessoais provenientes de ensaios clínicos conduzidos na UE a reguladores nos Estados Unidos, para efeitos de regulamentação e supervisão. Esse tipo de tranferência é permitido a outras partes para além dos reguladores, como instalações de empresas e outros investigadores?*

R 4: Sim, no respeito dos princípios de aviso e de escolha.

Q 5: *Para garantir a objectividade, em muitos ensaios clínicos, os participantes — e, frequentemente, também os investigadores — não têm acesso a informação sobre o tratamento que cada participante está a receber. Autorizar esse acesso comprometeria a validade do estudo e dos resultados da investigação. Irão os participantes nesses ensaios clínicos (denominados estudos «cegos») ter acesso a dados sobre o seu tratamento durante o ensaio?*

R 5: Não, esse acesso não tem de ser fornecido a um participante, se essa limitação tiver sido explicada quando o mesmo aderiu ao ensaio; a divulgação dessa informação comprometeria a integridade do esforço de investigação. O assentimento em participar no ensaio nestas condições constitui já uma renúncia razoável ao direito de acesso. No seguimento da conclusão do ensaio e da análise dos resultados, os participantes devem poder ter acesso aos dados que lhes dizem respeito, se o solicitarem. Devem solicitá-los, em primeiro lugar, ao médico ou prestador de serviços de saúde de quem receberam tratamento no âmbito do ensaio clínico ou, em seguida, à empresa patrocinadora.

Q 6: *Uma empresa de dispositivos farmacêuticos ou médicos tem de aplicar os princípios de «porto seguro» no que diz respeito ao aviso, à escolha, à re-transferência e ao acesso nas suas actividades de controlo da segurança e da eficácia do produto, incluindo a notificação de episódios adversos e o rastreio dos pacientes/pessoas em causa que utilizam certos medicamentos ou dispositivos médicos (por exemplo,* pacemakers)?

R 6: Não, desde que a adesão aos princípios não interfira com a observância dos requisitos regulamentares. Isto é válido tanto para as notificações efectuadas, por exemplo, pelos prestadores de cuidados de saúde às empresas de dispositivos farmacêuticos e médicos, como para as notificações efectuadas por estas empresas aos organismos governamentais como a Food and Drug Administration.

Q 7: *Invariavelmente, os dados da investigação são codificados, na sua origem, com uma chave única pelo investigador principal, de modo a não revelar a identidade das pessoas em causa. As empresas farmacêuticas que patrocinam essa investigação não recebem a chave. O código original é conhecido apenas pelo investigador, pelo que apenas este pode identificar a pessoa em causa em circunstâncias especiais (por exemplo, quando é necessário um acompanhamento médico). Uma transferência de dados codificados desta forma, da UE para os EUA, constitui um caso de transferência de dados pessoais sujeita aos princípios de «porto seguro»?*

R 7: Não, não se trata de uma transferência de dados pessoais sujeita aos referidos princípios.

FAQ 15 — Registos públicos e informação disponível ao público

Q: *Será necessário aplicar os princípios de aviso, escolha e re-transferência à informação de registos públicos ou à informação disponível ao público?*

R: Não é necessário aplicar os princípios de aviso, escolha ou re-transferência à informação de registos públicos, se estes não estiverem combinados com informação não pública, e desde que se respeitem as condições de consulta estabelecidas pela jurisdição pertinente.

Aliás, em geral, não é necessário aplicar os princípios de aviso, escolha e re-transferência à informação disponível ao público, excepto se o responsável europeu da transferência indicar que tal informação é objecto de restrições que exigem a aplicação desses princípios pela organização que se propõe utilizá-la. As organizações não são responsáveis da utilização dada à informação uma vez publicada.

Quando se verificar que uma organização divulgou intencionalmente informação pessoal em violação dos princípios, em benefício de si própria ou de terceiros, a sua participação deixará de ser aceite no «porto seguro».

ANEXO III

«Porto seguro»: Resumo das modalidades e aplicação

Autoridade federal e estadual em matéria de «práticas desleais e desonestas» e vida privada

O presente memorando explica a autoridade da Federal Trade Commission (FTC), instituída pela Section 5 da lei Federal Trade Commission Act (15 U.S.C. §§ 41-58, alterado), para tomar medidas contra as organizações que, contrariamente ao que anunciam ou em desrespeito dos princípios a que aderem, não respeitam as normas de protecção da vida privada aplicáveis às informações pessoais. Nele se analisam ainda as situações de excepção a essa autoridade e as competências de outras entidades públicas, federais e estaduais, para agir nesses casos [1].

Autoridade da FTC em matéria de práticas desleais ou desonestas

A Section 5 da lei Federal Trade Commission Act considera ilegais as «práticas ou actos desleais ou desonestos praticados no comércio ou que nele se reflectem», 15 U.S.C. § 45(a)(1). A mesma norma confere à FTC poderes para actuar contra tais actos e práticas, 15 U.S.C. § 45(a)(2). A FTC pode, segundo a lei e após audiência formal, emitir uma decisão administrativa para fazer «cessar e proibir» as referidas práticas, 15 U.S.C. § 45(b). Se for do interesse público, a FTC pode também procurar obter do tribunal distrital uma restrição temporária ou uma injunção temporária ou permanente, 15 U.S.C. § 53(b). Caso este tipo de práticas se verifique de forma generalizada, ou tenham já sido objecto de decisões administrativas para as fazer cessar e proibir, a FTC pode promulgar uma norma administrativa proibindo os actos ou práticas em causa, 15 U.S.C. § 57a.

O desrespeito da decisão da FTC poderá ser punido com multa até 11 000 USD, considerando-se que cada dia de violação continuada constitui em si mesmo nova violação [2], 15 U.S.C. § 45 (1). Da mesma forma, a violação consciente das regras da FTC poderá ser punida com 11 000 USD, 15 U.S.C. § 45(m). As medidas de aplicação podem ser decididas pelo Department of Justice ou pela FTC, em caso de impossibilidade do primeiro, 15 U.S.C. § 56.

Autoridade da FTC e protecção da vida privada

No exercício da autoridade que lhe incumbe por força da Section 5, a FTC considera prática enganosa a prestação ao consumidor de informação falsa ou incorrecta sobre as finalidades da recolha de dados no consumidor ou a sua utilização [3]. Em 1998, por exemplo, a FTC apresentou queixa contra GeoCities por esta organização ter divulgado a terceiros com fins comerciais informação recolhida no seu sítio *Web* sem consentimento prévio, apesar das suas declarações em contrário [4]. A FTC conclui ainda que a recolha de informação pessoal junto de crianças, e a sua comercialização e publicação sem consentimento parental, pode também ser considerada prática desleal [5].

---

[1] Não discutimos aqui as várias leis federais sobre protecção da vida privada em contextos específicos ou as leis estaduais e o direito consuetudinário que se poderia aplicar. As leis federais sobre recolha e uso comercial de informação pessoal incluem a Cable Communications Policy Act (47 U.S.C. § 551), a Driver's Privacy Protection Act (18 U.S.C. § 2721), a Electronic Communications Privacy Act (18 U.S.C. § 2701 et seq.), a Eletronic Funds Transfer Act (15 U.S.C. §§ 1693, 1693m), a Fair Credit Reporting Act (15 U.S.C. § 1681 et seq.), Right to Financial Privacy Act (12 U.S.C. § 3401 et seq.), a Telephone Consumer Protection Act (47 U.S.C. § 227), e a Video Privacy Protection Act (18 U.S.C. § 2710), entre outras. Muitos Estados têm legislação análoga nestas áreas. Ver, por exemplo, Mass. Gen. Laws ch. 167B, § 16 (proíbe às instituições financeiras a divulgação a terceiros de registos relativos a clientes, sem o consentimento destes ou justificação legal), N.Y. Pub. Health Law § 17 (limita o uso e a divulgação de ficheiros médicos e da saúde mental e dá aos pacientes o direito de acesso aos mesmos).

[2] Neste tipo de acção, os tribunais distritais dos EUA podem ordenar medidas provisórias e equitativas para fazer cumprir a decisão da FTC, 15 U.S.C. § 45(1).

[3] «Prática enganosa» define-se como representação, omissão ou prática susceptível de induzir em erro um consumidor razoável.

[4] Ver www.ftc.gov/opa/1998/9808/geocitie.htm.

[5] Ver carta a Center for Media Education, www.ftc.gov/os/1997/9707/cenmed.htm. Além disso, a lei Children's Online Privacy Protection Act de 1998 confere à FTC autoridade legal específica para regular a recolha de informação pessoal junto de crianças através da internet e por operadores de serviços em linha. Ver 15 U.S.C. §§ 6501-6506. Em particular, a lei exige dos operadores em linha que avisem e obtenham autorização parental antes de recolher, usar ou divulgar informação pessoal junto de crianças, *id*., § 6502(b). A lei dá ainda aos pais o direito de acesso e a possibilidade de impedir que a informação continue a ser utilizada, *id*.

Em carta dirigida a John Mogg, director-geral da Comissão Europeia, o Presidente Pitofsky da FTC destacou as limitações de autoridade da FTC para proteger a vida privada, sempre que não exista prestação de falsas declarações (ou não sejam prestadas quaisquer declarações) quanto à utilização da informação recolhida, carta do Presidente Pitofsky da FTC a John Mogg (23 de Setembro de 1998). Contudo, as empresas que pretendam usufruir dos benefícios do «porto seguro» deverão certificar que protegem a informação por si recolhida, de acordo com as directrizes previstas. Consequentemente, sempre que uma empresa viola as declarações de protecção da vida privada por si prestadas, incorre em prática de declarações falsas e «prática enganosa», na acepção da Section 5.

Uma vez que a jurisdição da FTC abarca as práticas e os actos desleais ou desonestos «praticados no comércio ou que nele se reflectem», a FTC não terá jurisdição sobre a recolha e o uso de informação pessoal para fins não comerciais, como os relacionados com a angariação de fundos para instituições de solidariedade social, por exemplo. Ver carta do Presidente Pitofsky, página 3. Contudo, qualquer transacção que utilize informação pessoal satisfaz este requisito jurisdicional, como é o caso da venda por um empregador de dados pessoais sobre os seus empregados a empresas de marketing directo, que já seria abarcada pelas disposições da Section 5.

Excepções à Section 5

A Section 5 determina as excepções à autoridade da FTC em matéria de práticas ou actos desleais ou desonestos relativamente a:

— instituições financeiras, incluindo bancos, instituições de poupança e crédito e cooperativas de crédito,

— redes de telecomunicações e sociedades de transportes interestaduais,

— transportadoras aéreas, e

— carregadores e entrepostos.

Ver 15 U.S.C. § 45(a)(2). As excepções e as respectivas autoridades de regulamentação são individualmente comentadas em seguida.

Instituições financeiras ([6])

A primeira excepção aplica-se a «bancos, instituições de poupança e crédito, descritos na section 18(f)(3) [15 U.S.C. § 57 a(f)(3)]» e «cooperativas de crédito federais descritas na section 18(f)(4) [15 U.S.C. § 57a(f)(4)]» ([7]). Estas instituições financeiras são objecto de regulamentação emitida por outras entidades; respectivamente, Federal Reserve Board, Office of Thrift Supervision ([8]) e National Credit Union Administration Board, ver 15 U.S.C. § 57a(f). Estas agências regulamentares podem emitir as normas necessárias para prevenir as práticas desleais e desonestas das referidas instituições financeiras ([9]) e oferecem um serviço separado para tratar queixas dos consumidores, 15 U.S.C. § 57a(f)(1). Por fim, a autoridade de aplicação deriva da section 8 de lei Federal Deposit Insurance act (12 U.S.C. § 1818), no que respeita a bancos, instituições de poupança e crédito, e das sections 120 e 206 da lei Federal Credit Union Act, no que concerna as cooperativas de crédito federais, 15 U.S.C. §§ 57a(f)(2)-(4).

Embora a indústria dos seguros não esteja especificamente incluída na lista de excepções da Section 5, a lei McCarran-Ferguson Act (15 U.S.C. § 1011 et seq.) geralmente deixa a regulamentação dos seguros ao cuidado dos Estados indivi-

([6]) Em 12 de Novembro de 1999, o Presidente Clinton promulgou a lei Gramm-Leach-Bliley Act (Pub. L. 106-102, codificada em 15 U.S.C. § 6801 et seq.), que limita a divulgação, pelas instituições financeiras, de informação pessoal sobre os clientes e exige que as referidas instituições notifiquem, *inter alia*, todos os clientes da sua política e prática em matéria de protecção da vida privada, no que diz respeito à partilha de informação pessoal com filiais e outros organismos. A lei autoriza a FTC, as autoridades bancárias federais e outras entidades a emitir regulamentação para implementar as medidas de protecção da vida privada exigidas pela lei. As agências emitiram propostas de regulamentação com este fim.

([7]) As suas disposições determinam que esta excepção não se aplica ao sector das sociedades de valores. Assim, os corretores, intermediários e outros agentes do sector estão sujeitos a jurisdição concorrente da Securities and Exchange Commission e da FTC no que diz respeito a actos e práticas desleais e desonestos.

([8]) A excepção prevista na Section 5 originalmente referia-se ao Federal Home Loan Bank Board abolido em Agosto de 1989 pela lei Financial Institutions Reform, Recovery and Enforcement Act de 1989, cujas funções foram transferidas para o Office of Thrift Supervision, Resolution Trust Corporation, a Federal Deposit Insurance Corporation, e a Housing Finance Board.

([9]) Embora afaste as instituições financeiras da jurisdição da FTC, a Section 5 estipula que sempre que a FTC emite regras sobre práticas e actos desleais e desonestos, os organismos de regulamentação financeira devem adoptar medidas parelelas no prazo de 60 dias, ver 15 U.S.C. § 57a(f)(1).

duais ([10]). Além disso, segundo a section 2(b) da lei McCarran-Ferguson Act, nenhuma lei federal poderá invalidar, afectar ou substituir a regulamentação estadual «a não ser que especifique claramente o sector dos seguros», 15 U.S.C. § 1012(b). Contudo, as disposições da FTC Act abrangem a indústria dos seguros «na medida em que essa actividade não for regulamentada por legislação estadual», *id*. Deveria ainda destacar-se que a lei McCarran-Ferguson Act só delega nos Estados em matéria de «actividades de seguros», mantendo, assim, a FTC alguma autoridade em matéria de práticas desleais ou desonestas verificadas nas companhias de seguros sim, mas não relacionadas com actividades seguradoras. Isto poderia incluir casos em que o vendedor vende informações pessoais sobre os seus clientes a empresas de marketing directo de produtos não relacionados com os seguros, por exemplo ([11]).

Sociedades de Transportes

A segunda excepção da Section 5 abarca as sociedade de transportes «sujeitas às leis de regulamentação do comércio», 15 U.S.C. § 45(a)(2). Neste caso, as «leis de regulamentação do comércio» referem-se ao subtitle IV do Title 49 do United States Code e à lei Communications Act de 1934 (47 U.S.C. § 151 et seq.) (Communications Act), ver 15 U.S.C. § 44.

A referida lei (49 U.S.C. subtitle IV) (Interstate Transportation) sobre transportes interestaduais abrange os transportadores ferroviários, rodiviários, por vias navegáveis, agentes, transitários e transportadores por oleodutos, 49 U.S.C. § 10101 et seq. Estes transportadores, conquanto diversos, estão sujeitos a regulamentação do Surface Transportation Board, uma agência independente do Department of Transportation, 49 U.S.C. §§ 10501, 13501, e 15301. Em todos os casos, a lei federal proíbe aos transportadores a divulgação de informações sobre a natureza, o destino, e outros aspectos da carga transportada que possam ser utilizadas em detrimento do expedidor, ver 49 U.S.C. §§ 11904, 14908, e 16103. Note-se que estas disposições se referem à cargo do expedidor e não às informações pessoais sobre o expedidor propriamente dito, irrelevantes para a carga em questão.

Tal como a lei Communications Act, a Federal Communications Commission (FCC) regula o «comércio interestatal e estrangeiro nas comunicações por cabo e por rádio», ver 47 U.S.C. §§ 151 e 152. Além das empresas públicas de telecomunicações, a lei Communications Act também se aplica a empresas de televisão e rádio, e a fornecedores de serviços por cabo que não se consideram empresas públicas. Como tal, estas últimas empresas não se incluem nas excepções pevistas na Section 5 da FTC Act e, por isso, tem a FTC jurisdição para as investigar em matéria de práticas desleais ou desonestas, complementada pela da FCC que pode aplicar a sua autoridade independente nesta área, como a seguir se descreve.

Ao abrigo da lei Communications Act, «todas as empresas de telecomunicações», incluindo os intermediários locais, têm o dever de proteger a vida privada e as informações específicas dos seus clientes ([12]), 47 U.S.C. § 222(a). Além desta autoridade geral em matéria de protecção da vida privada, a lei Communications Act foi alterada pela lei Cable Communications Policy de 1984 (Cable Act), 47 U.S.C. § 521 et seq., para assegurar especificamente que os operadores de cabo protejam a vida privada, no caso da «informação pessoalmente identificável» dos assinantes, 47 U.S.C. § 551 ([13]). A lei Cable Act limita a recolha de informação pessoal pelos operadores de cabo e exige que estes notifiquem o assinante da natureza da informação recolhida e dos fins a que se destina. A lei dá aos assinantes o direito de acederem à sua informação pessoal e exige dos operadores de cabo que a destruam quando deixa de ser necessária.

A lei Communications Act confere à FCC poder para aplicar estas duas disposições em matéria de protecção da vida privada, quer por sua própria iniciativa, quer em resposta a uma queixa vinda do exterior ([14]) 47 U.S.C. §§ 205, 403; *id*. § 208. Se a FCC determinar que uma empresa de telecomunicações (incluindo um operador de cabo) violou a vida

([10]) «Os seguros e todos os que exercem a sua actividade nesse sector estarão sujeitos às leis de vários Estados relacionadas com a regulamentação ou fiscalidade do sector», 15 U.S.C. § 1012(a).

([11]) A FTC exerceu a sua jurisdição sobre companhias de seguros em diferentes ocasiões, incluindo um caso em que tomou medidas contra uma companhia por publicidade enganosa num Estado onde não tinha autorização para exercer a sua actividade. A jurisdição da FTC foi aceite com base no facto de não existir regulamentação realmente eficaz dado que a companhia se encontrava fora do alcance da legislação desse Estado, ver FTC v. Travelers Health Association, 362 U.S. 293 (1960).
Quanto aos Estados, 17 adoptaram o modelo da lei «Insurance Information and Privacy Protection Act» preparado pela National Association of Insurance Commissioners (NAIC). A lei inclui disposições em matéria de aviso, uso e divulgação, e acesso. Quase todos os Estados adoptaram o modelo da NAIC «Unfair Insurance Practices Act» que especifica as práticas comerciais desleais seguidas na indústria dos seguros.

([12]) O termo «rede de propriedade reservada dos utentes» significa informação relacionada com «a quantidade, a configuração técnica, o tipo, o destino e a frequência do uso de um serviço de telecomunicações» por um cliente e informação de facturas telefónicas, 47 U.S.C. § 222(f)(1). Contudo, o termo não inclui informação das listas de assinantes, *id*.

([13]) A legislação não define expressamente «informação pessoal identificável».

([14]) Esta autoridade inclui o direito de reparação, em caso de violação da vida privada, ao abrigo da section 222 da lei Comunications Act ou, no caso dos assinantes de serviços por cabo, ao abrigo da section 551 da lei Cable Act, com as respectivas alterações, ver ainda 47 U.S.C. § 551(f)(3) (uma acção civil no tirbunal federal de distrito é um dos remédios possíveis, «além das outras soluções juridicamente disponíveis aos assinantes dos serviços por cabo»).

privada, na acepção das disposições da section 222 ou section 551, pode tomar três tipos de medidas. Primeiro, após inquérito para determinar a violação, a Commission pode ordenar à empresa que pague danos monetários ([15]) 47 U.S.C. § 209. Alternativamente, a FCC pode fazer cessar e proibir a referida prática ou omissão, 47 U.S.C. § 205(a). Finalmente, a Commission pode também ordenar a uma empresa em falta que «respeite e cumpra (quaisquer) regulamentos ou práticas» que a FCC possa decidir, *id*.

Qualquer pessoa que considere que existe violação das disposições da lei Communications Act ou Cable Act por parte de empresas de telecomunicações ou operadores de cabo pode apresentar queixa à FCC ou a um tribunal federal do distrito, 47 U.S.C. § 207. O queixoso que ganhar a acção em tribunal federal contra uma empresa de telecomunicações acusada de não proteger a informação específica dos seus clientes, nos termos da section 222 da lei Communications Act, poderá receber ressarcimento pelos danos sofridos e ver reembolsados os honorários dos seus advogados, 47 U.S.C. § 206. Um queixoso que apresente uma queixa por violação da vida privada, segundo as disposições específicas da section 551 da lei Cable Act poderá, além de receber ressarcimento pelos danos sofridos e ver reembolsados os honorários dos seus advogados, receber indemnizações e custos processuais razoáveis, 47 U.S.C. § 551(f).

A FCC tem adoptado regras pormenorizadas para implementar a section 222, ver 47 CFR 64.2001-2009. Estas regras estipulam garantias específicas contra acesso não autorizado a redes de propriedade reservada dos utentes e exigem das empresas de telecomunicações que:

— desenvolvam e implementem sistemas de *software* capazes de «assinalar» o aviso/aprovação de um cliente no ficheiro que surge no ecrã pela primeira vez,

— mantenham um «registo de auditoria» electrónico para assinalar as consultas às contas dos clientes, incluindo dados sobre abertura do ficheiro, por quem e com que fins,

— treinem o seu pessoal sobre os usos autorizados das informações sobre a rede de propriedade reservada dos utentes, incluindo os adequados processos disciplinares,

— estabeleçam procedimentos de supervisão por forma a garantir o cumprimento das operações de marketing externo, e

— certifiquem anualmente à FCC as formalidades de cumprimento dessas regras.

Transportadoras aéreas

As transportadoras aéreas americanas e estrangeiras sujeitas à lei Federal Aviation Act de 1958 estão igualmente excluídas das disposições da Section 5 da FTC Act, ver 15 U.S.C. § 45(a)(2). Nesta categoria incluem-se os transportes interestaduais ou estrangeiros de passageiros ou mercadorias, ou de correio, por avião, ver 49 U.S.C. § 40102. As transportadoras aéreas estão sob a alçada do Department of Transportation, e quanto a isto, o Secretary of Transportation está autorizado a tomar medidas para «evitar práticas desleais, desonestas, predatórias ou anticoncorrenciais nos transportes aéreos», ver 49 U.S.C. § 40101(a)(9). Quando se tratar do interesse público, esta entidade pode investigar as práticas supostamente desleais ou desonestas de transportadoras aéreas americanas ou estrangeiras, ou de agências de viagens, ver 49 U.S.C. § 41712. Após audiência, pode ainda decidir a cessação da prática ilegal, *id*. Porém, segundo nos é dado saber, a referida entidade ainda nunca exerceu a sua autoridade no âmbito da protecção da vida privada de clientes de transportadoras aéreas ([16]).

São duas as disposições destinadas a proteger a informação privada aplicáveis às transportadoras aéreas em contextos específicos. Em primeiro lugar, a lei Federal Aviation Act, que protege a vida privada dos candidatos a piloto, ver 49 U.S.C. § 44936(f). Conquanto permitindo às transportadoras obter os registos de emprego do candidato, a lei concede a este último o direito a ser avisado desse facto e de dar o seu consentimento para tal, de corrigir inexactidões e de ver os seus registos divulgados apenas aos responsáveis pelo recrutamento. Em segundo lugar, as regulamentações do DOT exigem que as informações recolhidas sobre os passageiros para uso governamental em caso de desastre aéreo «sejam mantidas confidenciais e divulgadas só ao U.S. Department of State, ao National Transportation Board (mediante pedido do NTSB), e ao U.S. Department of Transportation», 14 CFR parte 243, § 243.9(c) (conforme alteração de 63 FR 8258).

([15]) Contudo, a ausência de danos directos a um queixoso não constitui motivo para não aceitar a queixa, 47 U.S.C. § 208(a).

([16]) Compreendemos que estão a ser enviados esforços pela indústria no sentido de resolver o aspecto da protecção da vida privada. Os representantes da indústria discutiram os princípios de «porto seguro» e a sua possível aplicação às transportadoras aéreas. A discussão incluiu uma proposta para que a indústria adopte uma política nesta matéria, ficando as empresas participantes expressamente submetidas à autoridade do DOT.

Carregadores e Entrepostos

A lei de 1921 sobre Packers and Stockyards (7 U.S.C. § 181 et seq.), considera ilegais «as práticas ou os equipamentos desleais, injustamente discriminatórios ou desonestos, praticados ou usados por carregadores e relacionados com gado, carne, produtos alimentares de origem animal ou produtos animais não transformados, ou por comerciantes de aves e relacionados com aves vivas», 7 U.S.C. § 192(a); ver ainda 7 U.S.C. § 213(a) (proíbe «as práticas e os equipamentos desleais, injustamente discriminatórios ou desonestos» relacionados com gado). Cabe ao Secretary of Agriculture a responsabilidade primeira de aplicar estas disposições, enquanto à FTC pertence a jurisdição sobre transacções no comércio retalhista e as que envolvem a indústria avícola, 7 U.S.C. § 227(b)(2).

Não é claro se o Secretary of Agriculture poderá interpretar o desrespeito de carregadores e entrepostos pela protecção da vida privada de acordo com a política declarada como um prática *desleal*, ao abrigo da lei sobre carregadores e entrepostos. Contudo, a excepção à Section 5 aplica-se a pessoas, parcerias ou empresas na medida em que «estejam sujeitas à lei Packers and Stockyards Act». Assim, se a protecção da vida privada não é um assunto abrangido pela Packers and Stockyards Act, a excepção da Section 5 poderá não se aplicar, ficando os carregadores e entrepostos sujeitos à autoridade da FTC nessa matéria.

Autoridade estadual competente em matéria de «Práticas desleais e desonestas»

Segundo uma análise preparada pela FTC, publicada no boletim daquela entidade e retomada em Comment, Consumer Protection: The Practical Effectiveness of State Deceptive Trade Practices Legislation, 59 Thul. L. Rev. 427 (1984), «os cinquenta estados mais o District of Columbia, Guam, Porto Rico, e as Ilhas Virgens promulgaram legislação semelhante à Federal Trade Commission Act ("FTCA") para prevenir os actos desleais ou desonestos». Em todos os casos, existe um organismo de aplicação com autoridade para «investigar e aplicar sanções ou decisões de investigação, obter compromissos de cumprimento voluntário, fazer cessar e proibir essas práticas e obter despachos judiciais para evitar o uso de práticas comerciais desleais ou desonestas», *id*. Em 46 jurisdições as pessoas podem intentar acções em tribunal visando a obtenção de indemnizações simples, duplas, triplas ou compensatórias e, em alguns casos, recuperação de custos processuais e honorários de advogados, *id*.

A lei da Florida, Deceptive and Unfair Trade Practices Act, por exemplo, permite investigar e interpor recurso contra «métodos desleais de concorrência, e práticas comerciais desleais ou desonestas», incluindo publicidade falsa ou enganosa, franquiamentos ou oportunidades de negócios enganosos, telemarketing fraudulento e vendas em pirâmide. Ver ainda N.Y. General Business Law § 349 (proíbe os factos desleais e as práticas desonestas no domínio das actividades comerciais).

Um inquérito efectuado pela National Association of Attorneys General (NAAG) confirma estas conclusões. Todos os 43 estados inquiridos possuem leis do tipo FTC ou outras equiparadas em termos de protecção; desses, 39 indicaram ter competência para receber queixas de não residentes. Quanto à protecção da vida privada do consumidor, em particular, 37 Estados disseram estar dispostos a aceitar queixas contra empresas da sua jurisdição que não cumpram as declarações efectuadas em matéria de protecção da vida privada.

ANEXO IV

Memorando sobre danos por violação das regras de protecção da vida privada e autorizações explícitas na legislação dos EUA

O presente documento responde ao pedido apresentado pela Comissão Europeia, de clarificação da legislação dos Estados Unidos da América em matéria de a) queixas por quebra da privacidade, b) «autorizações explícitas» na legislação dos EUA no que respeita ao uso de informação pessoal de forma incoerente com os princípios de «porto seguro», e c) efeitos das fusões e aquisições nos compromissos decorrentes do «porto seguro».

A. **Danos resultantes da quebra da privacidade**

O incumprimento dos princípios de «porto seguro» pode dar origem a diversas queixas privadas, consoante as circunstâncias. Em particular, as organizações aderentes ao «porto seguro» podem ser acusadas de prestar falsas declarações se não respeitarem as respectivas políticas de protecção da vida privada. O direito consuetudinário também possibilita a interposição de acções por violação da legislação em matéria de protecção da vida privada. Muitas normas federais e estaduais em matéria de vida privada prevêem igualmente ressarcimento de danos por pessoas de direito singular em caso de violação dessas regras.

O direito a ressarcimento de danos por violação da vida privada está bem enraizado no direito consuetudinário norte-americano.

De acordo com várias teorias jurídicas, a utilização de informação pessoal de maneira incompatível com os princípios de «porto seguro» poderá levantar problemas de responsabilidade civil. Por exemplo, tanto o responsável pelo tratamento e transferência dos dados, como as pessoas em causa, poderão processar por declarações falsas a organização aderente ao «porto seguro» que não cumpra os compromissos declarados nesta matéria. De acordo com o Restatement of the Law, Second, Torts ([1]):

> Quem apresentar falsas informações sobre factos, opiniões, intenções ou legislação, com o objectivo de levar terceiros a agir ou a abster-se de agir em função dessas informações, é civilmente responsável pelas perdas pecuniárias dessa pessoa sofridas em resultado do crédito atribuído a tais declarações.

Restatement, § 525. Uma informação falsa é «fraudulenta» quando é facultada com o conhecimento ou a consciência de que é falsa, *id.*, § 526. Em regra geral, o responsável por tais declarações falsas é potencialmente responsável perante todos os que sofrerem perdas pecuniárias resultantes dessa credibilidade, *id.*, § 531. Além disso, quem apresentar falsas declarações pode ser responsabilizado perante terceiros se a declaração for efectuada na intenção de ser repetida de boa fé, *id.*, § 533.

No contexto do «porto seguro», a declaração relevante é a que a organização efectua publicamente segundo a qual adere aos princípios de «porto seguro». Uma vez assumido tal compromisso, a quebra voluntária do respeito dos princípios poderá constituir fundamento para interposição de acções por falsas declarações por quem nelas tenha confiado. Visto que o compromisso de aderir aos princípios é público, as pessoas em causa, bem como os responsáveis pelo tratamento dos dados na Europa que transferem informações de carácter pessoal para a organização dos EUA, terão todas as razões para moverem acções contra essa mesma organização por falsas declarações ([2]). Além do mais, a organização dos EUA permanece responsável pela continuação das «falsas declarações» enquanto as pessoas forem prejudicadas por elas, Restatement, § 535.

([1]) Second Restatement of the Law — Torts; American Law Institute (1997).

([2]) Poderia ser o caso, por exemplo, em que as pessoas confiem nos compromissos assumidos pela organização norte-americana em relação ao «porto seguro», ao darem o seu consentimento para que a sua informação pessoal seja transferida pelo responsável pelo tratamento de dados para os EUA.

Quem confiar em declarações falsas terá o direito a ressarcimento. De acordo com o Restatement:

> O destinatário de uma declaração falsa está autorizado a recuperar, sob forma de indemnização, a perda pecuniária que o autor da declaração tenha juridicamente causado.

Restatement, § 549. Os danos podem incluir perdas correntes ou perdas dos «benefícios do negócio» de uma transacção comercial, *id.*; ver, por exemplo, Boling v. Tennessee State Bank, 890 S.W.2d 32 (1994) (banco compensa em 14 825 USD os clientes de um empréstimo por ter divulgado informação pessoal e planos comerciais ao presidente do banco cujos interesses eram conflituais).

Enquanto a declaração fraudulenta requer conhecimento factual ou pressuposto, pelo menos, de que a declaração é falsa, a responsabilidade pode limitar-se à negligência das declarações. De acordo com o Restatement, quem quer que preste declarações falsas no contexto das suas actividades comerciais, profissionais ou laborais, ou de qualquer transacção pecuniária, poderá ser responsabilizado «se não demonstrar cuidado ou competência razoáveis na obtenção ou na comunicação da informação». Restatement, § 552(1). Contrariamente ao que acontece em caso de declaração fraudulenta, o ressarcimento por danos devidos a declaração negligente limita-se a perdas pouco elevadas. *id.*, § 552B(1).

Num caso recente, por exemplo, o Supremo Tribunal do Connecticut decidiu que o facto de um serviço de electricidade não ter informado que divulgava informações sobre os pagamentos dos clientes a agências de crédito nacionais justificava uma acção por declarações falsas. Ver Brouillard v. United Illuminating Co., 1999 Conn. Super. LEXIS 1754. Nesse caso, o arguido negou crédito ao queixoso, que efectuou pagamentos «em atraso», além dos 30 dias previstos pela factura. O queixoso alegou que não tinha sido informado dessa condição aquando da abertura de uma conta junto da companhia de electricidade. O tribunal decidiu especificamente que «uma queixa por declarações negligentes podia basear-se no facto de o arguido não ter prestado os esclarecimentos devidos na altura devida». Este caso mostra ainda que o facto de agir de boa fé ou a intenção fraudulenta não são elementos necessários numa acção por declarações negligentes. Assim, uma organização norte-americana que por negligência não presta todas as informações sobre a forma como irá utilizar as informações recebidas ao abrigo do «porto seguro» poderá ser responsabilizada por prestar declarações falsas.

Na medida em que a violação dos princípios de «porto seguro» comporte uma utilização incorrecta de informações pessoais, pode também justificar uma queixa da pessoa em questão pelo delito de violação da vida privada previsto no direito consuetudinário. O direito norte-americano há muito reconhece acções relacionadas com a invasão da vida privada. Num caso de 1905 ([3]), o Supremo Tribunal da Georgia reconheceu que o direito à vida privada radica nos preceitos do direito natural e consuetudinário, ao julgar o caso de um cidadão cuja fotografia tinha sido utilizada por uma companhia de seguro de vida, sem o seu consentimento ou conhecimento, para ilustrar um anúncio comercial. Utilizando temas recorrentes na jurisprudência norte-americana sobre protecção da vida privada, o tribunal considerou que a utilização da fotografia era «maliciosa», «falsa» e procurava «ridicularizar o queixoso aos olhos do mundo» ([4]). Os fundamentos do acórdão Pavesich prevaleceram com pequenas variações e transformaram-se nas bases do direito norte-americano nesta matéria. Os tribunais nacionais julgam constantemente casos de violação da vida privada, e pelo menos 48 Estados reconhecem agora judicialmente um tal fundamento para agir ([5]). Além disso, pelo menos 12 Estados têm disposições constituicionais de salvaguarda dos direitos dos seus cidadãos contra a violação da vida privada ([6]), que em alguns casos se podem alargar à protecção contra a intrusão por parte de entidades não governamentais, ver, por exemplo, Hill v. NCAA, 865 P.2d 633 (Ca. 1994); ver ainda Ginder, Lost and Found in Cyberspace: Informational Privacy in the Age of the Internet, 34 S.D. L. Rev. 1153 (1997) («algumas constituições estaduais incluem disposições de protecção da vida privada mais exigentes do que as da própria constituição nacional dos EUA. Alaska, Arizona, California, Florida, Hawai, Illinois, Louisiana, Montana, South Carolina, e Washington estão neste último caso»).

O Second Restatement of Torts propõe uma visão fundamentada do direito relativo a esta área. Reflectindo a prática comum, o Restatement explica que o «direito à vida privada» engloba quatro tipos de acção por incumprimento, ver Restatement, § 652A. Em primeiro lugar, a acção por «ingerência na vida privada» pode ser utilizada contra um arguido que intencionalmente viole, fisicamente ou por outros meios, a vida privada ou os interesses privados de um outro

([3]) Pavesich v. New England Life Ins. Co., 50 S.E. 68 (Ga. 1905).

([4]) *Id.*, em 69.

([5]) Uma pesquisa electrónica na base de dados Westlaw encontrou 2 703 acções em tribunais estaduais por razões de quebra da privacidade, desde 1995. Anteriormente apresentámos o resultado desta pesquisa à Comissão.

([6]) Ver, por exemplo, Alaska Constitution, artigo 1, secção 22; Arizona, artigo 2, secção 8; California, artigo 1, secção 1; Florida, artigo 1, secção 23; Hawaii, artigo 1, secção 5; Illinois, artigo 1, secção 6; Louisiana, artigo 1, secção 5; Montana, artigo 2, secção 10; New York, artigo 1, secção 12; Pennsylvania, artigo 1, secção 1; South Carolina, artigo 1, secção 10; e Washington, artigo 1, secção 7.

cidadão ([7]). Em segundo lugar, podemos estar perante um caso de «apropriação» quando alguém usurpar o nome ou o aspecto de um outro para seu próprio uso ou benefício ([8]). Em terceiro lugar, a «publicação de factos privados» é passível de ser levada a tribunal quando o assunto for de índole a ofender a pessoa em questão e não for do interesse legítimo do público ([9]). Por último, pode ser adequada uma acção por «difamação» quando o arguido consciente ou inconscientemente apresenta um outro ao público sob uma falsa luz, considerada difamatória por uma pessoa razoável ([10]).

No contexto do «porto seguro», a «ingerência na vida privada» pode englobar a recolha não autorizada de informação sobre a pessoa e a utilização não autorizada de informação para efeitos comerciais pode justificar uma acção por apropriação. Da mesma forma, a revelação de informação pessoal inexacta dará lugar a uma acção por «difamação» se a informação for considerada altamente ofensiva por uma pessoa razoável. Finalmente a invasão da vida privada que decorra de publicação ou divulgação de informação pessoal sensível poderá justificar uma acção por «publicação de factos privados» (ver exemplos de casos *infra*.)

Sobre o tema dos danos, a violação da vida privada dará ao lesado o direito a ressarcimento por:

a) O prejuízo infligido aos seus interesses resultante da violação;

b) O dano moral comprovado tipicamente resultante dessa mesma violação; e

c) Os danos especiais dos quais a violação seja um fundamento jurídico.

Restatement, § 652H. Dada a aplicabilidade geral das normas de responsabilidade civil e a multiplicidade de acções abrangendo diversos aspectos da protecção da vida privada, os danos monetários podem ser infligidos a quem sofre invasão dos seus interesses privados, como resultado da violação dos princípios do «porto seguro».

De facto, os tribunais estaduais estão repletos de casos de alegada violação da privacidade em situações análogas. Ex Parte AmSouth Bancorporation et al., 717 So. 2d 357, por exemplo, diz respeito a uma acção na qual o arguido «explorou os fundos colocados no banco pelos depositantes, sobre os quais divulgou informação confidencial bem como sobre as suas contas» para permitir a uma filial vender investimentos e outros produtos. Nestes casos, o ressarcimento é geralmente concedido. Em Vassiliades v. Garfinckel's, Brooks Bros., 492 A.2d 580 (D.C.App. 1985), um tribunal de recurso revogou uma sentença considerando que a utilização numa loja de fotografias do queixoso, «antes» e «depois» de uma cirurgia plástica, constituíam uma violação da vida privada, com publicação de factos privados. Em Candebat v. Flanagan, 487 So.2d 207 (Miss. 1986), a companhia de seguros do arguido usou um acidente em que a mulher do queixo ficou seriamente ferida para uma campanha publicitária. O queixoso processou-o por violação da privacidade. O tribunal decidiu que o queixoso seria ressarcido por danos morais e apropriação de identidade. As acções por apropriação de imagem podem ser intentadas ainda que o queixoso não seja famoso, ver, por exemplo, Staruski v. Continental Telephone Co., 154 Vt. 568 (1990) (o acusado obteve benefícios comerciais por utilizar o nome e a fotografia de um empregado num anúncio no jornal). Em Pulla v. Amoco Oil Co., 882 F.Supp. 836 (S.D Iowa 1995), um empregador violou a vida privada de um empregado, ao pôr outro empregado a investigar as facturas do cartão de crédito do primeiro, para verificar os dias de baixa por doença. O tribunal confirmou a decisão do júri de conceder 2 USD de indemnização corrente e 500 000 USD de indeminzação compensatória. Um outro empregado foi responsabilizado por publicar um artigo no jornal da empresa sobre um colega anteriormente despedido por alegadamente ter falsificado os respectivos registos de emprego, ver Zinda v. Louisiana-Pacific Corp., 140 Wis.2d 277 (Wis.App. 1987). Ao utilizar informação privada, o artigo violava a privacidade da pessoa em causa porque o jornal circulava na comunidade. Finalmente, uma universidade que efectuava análises aos alunos para despistar o HIV, dizendo-lhes que eram para despiste da rubéola, foi responsabilizada por violação da vida privada, ver Doe v. High-Tech Institute, Inc., 972 P.2d 1060 (Colo.App. 1998). (Para outros casos, ver Restatement, § 652H, Appendix).

Os EUA são frequentemente criticados pela sua tendência exagerada para o litígio, mas isto também significa que as pessoas podem, e fazem-no, recorrer à lei quando consideram ter sido vítimas de injustiça. Muitos aspectos do sistema

([7]) *Id.*, Chapter 28, Section 652B.
([8]) *Id.*, Chapter 28, Section 652C.
([9]) *Id.*, Chapter 28, Section 652D.
([10]) *Id.*, Chapter 28, Section 652E.

judical norte-americano facilitam a apresentação de queixas, quer individuais, quer em grupo. Os advogados, em número superior do que na maioria dos outros países, tornam a representação profissional imediatamente disponível. O advogado do quexoso, que representa pessoas em litígios privados, trabalha com base em honorários aleatórios, permitindo até a pessoas de menores recursos e sem recursos procurar reparação. Este aspecto é importante, visto que nos EUA cada uma das partes suporta os honorários dos seus advogados e outros custos, o que contrasta com a regra europeia, segundo a qual quem perde deve reembolsar os custos da outra parte. Sem discutir os méritos dos dois sistemas, a regra norte-americana é menos susceptível de dissuadir as pessoas sem recursos, que não poderiam suportar os custos de ambas as partes se perdessem, de apresentar queixas legítimas.

As pessoas podem procurar recuperar os seus danos, ainda que as suas queixas sejam de baixo valor pecuniário. Na maioria ou mesmo em todas as jurisdições norte-americanas existem pequenos tribunais destinados a receber queixas onde são tratados os litígios de valor pecuniário inferior a certos limites fixados na lei, de forma simplificada e menos onerosa ([11]). O potencial para ressarcimento de danos com valor compensatório oferece também uma recompensa financeira a pessoas que possam ter sofrido pequenos danos directos se instaurarem um processo por conduta repreensível. Finalmente, as pessoas que tenham sido vítimas do mesmo tipo de problema podem organizar os seus recursos e as suas queixas para intentar um processo em grupo.

Um bom exemplo da possibilidade de as pessoas intentarem processos para obterem ressarcimento é a acção pendente contra Amazon.com por violação da vida privada. Amazon.com, a grande empresa de vendas em linha, é objecto de uma acção por parte de um grupo de pessoas, em que o queixoso diz não ter sido informado nem ter consentido a recolha de dados pessoais aquando da utilização de um programa informático propriedade daquela empresa chamado «Alexa» Naquele caso, os queixosos alegaram violação da lei Computer Fraud and Abuse Act, por acesso às suas comunicações arquivadas e da lei Electronic Communications Privacy Act, por intercepção ilegal das suas comunicações electrónicas e telefónicas. Por outro lado, reclamaram ainda uma violação da privacidade segundo o direito consuetudinário. Isto deriva de uma queixa apresentada por um perito da segurança na internet em Dezembro. Neste processo são pedidos 1 000 USD de indemnização por cada pessoa, além dos honorários do advogado e lucros obtidos em resultado da violação das leis. Dado que as pessoas envolvidas podem cifrar-se em milhões, os danos poderão ascender a biliões de USD. A própria FTC está a investigar o caso.

A legislação federal e estadual sobre a vida privada oferece frequentemente fundamentos de acção por danos monetários.

Além de dar origem a responsabilidade civil no âmbito do direito civil, a não observação dos princípios do «porto seguro» pode ainda violar uma ou outra das centenas de normas federais e estaduais sobre a vida privada, muitas das quais, simultaneamente sobre o tratamento público e privado da informação pessoal, permitem às pessoas processar por danos decorrentes dessa mesma violação. Por exemplo:

Electronic Communications Privacy Act de 1986. Esta lei proíbe a intercepção não autorizada de comunicações de telefones celulares e entre computadores. As violações podem resultar em acções de responsabilidade civil não inferiores a 100 USD por cada dia de violação. A protecção da lei estende-se ainda ao acesso sem autorização ou à divulgação de comunicações electrónicas arquivadas. Os autores destes actos poderão ser responsabilizados pelos danos sofridos ou pelas consequências ou lucros derivados da operação.

Telecommunications Act de 1996. Segundo a secção 702 desta lei, as informações sobre a rede de propriedade reservada dos utentes (CPNI) não podem ser utilizadas para outros fins além do fornecimento de serviços de telecomunicações. Os assinantes do serviço podem apresentar queixa à Federal Communications Commission ou apresentar o caso ao tribunal federal da zona para ressarcimento de danos e honorários de advogado.

Consumer Credit Reporting Reform Act de 1996. Esta lei, de 1996, alterou o Fair Credit Reporting Act de 1970 (FCRA) para melhorar o direito de informação e de acesso dos sujeitos de informações comerciais. A lei impôs ainda novas restrições aos revendedores de informações comerciais sobre os consumidores que podem agora recuperar os honorários dos advogados e ser ressarcidos pelos danos sofridos.

([11]) Já informámos a Comissão sobre este tipo de acções.

A legislação estadual protege ainda a vida privada em várias outras situações, incluindo registos bancários, assinaturas de televisão por cabo, informações comerciais, registos laborais, arquivos públicos, informação genética e registos médicos, registos de companhias de seguros, arquivos escolares, comunicações electrónicas e aluguer de cassetes vídeo ([12]).

B. **Autorizações legais explícitas**

Os princípios de «porto seguro» contêm excepções nos casos em que uma lei, um regulamento ou a jurisprudência criem «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». Claramente, sempre que a legislação norte-americana impõe uma obrigação contraditória, as organizações norte-americanas, aderentes ou não ao «porto seguro» têm que aplicar a lei. Quanto às autorizações explícitas, enquanto os princípios de «porto seguro» se destinam a colmatar as diferenças entre os regimes europeus e norte-americanos de protecção da vida privada, devemos respeitar as prerrogativas legislativas dos nossos legisladores eleitos. A excepção limitada ao respeito rigoroso dos princípios de «porto seguro» procura equilibrar os interesses legítimos de ambas as partes.

A excepção limita-se a casos em que existe autorização explícita. Assim, em último caso, a lei relevante, o regulamento ou a decisão do tribunal devem autorizar especificamente essa conduta particular por parte das organizações do «porto seguro» ([13]). Por outras palavras, a excepção não se aplica quando a lei for omissa. Além disso, a excepção aplicar-se-á apenas se a autorização específica for contraditória com os princípios de «porto seguro». Mesmo então, a excepção não deverá ultrapassar o «necessário para respeitar os legítimos interesses superiores avançados por essa autorização». Como exemplo, pode dizer-se que quando a lei autoriza simplesmente uma empresa a fornecer informação pessoal às entidades públicas, a excepção não se aplica. Em contrapartida, quando a lei autorizar especificamente uma empresa a fornecer informação pessoal a agências governamentais sem o consentimento da pessoa, isto constituirá uma «autorização explícita» para agir de forma contraditória com os princípios do «porto seguro». Alternativamente, as excepções específicas às exigências afirmativas para fornecer aviso e obter consentimento seriam abrangidas pelo âmbito da excepção (uma vez que seriam equivalentes a uma autorização específica para divulgar informação sem aviso nem consentimento). Por exemplo, uma norma que autorize os médicos a divulgar aos serviços de saúde os *dossiers* dos seus pacientes, sem o consentimento prévio destes últimos, poderia permitir uma excepção aos princípios de aviso e escolha. Tal autorização não permitiria a um médico facultar os mesmos *dossiers* a organizações de saúde ou laboratórios farmacêuticos, não abrangidos pelo âmbito dos objectivos autorizados pela lei e, assim, não podem ser considerados excepção ([14]). A autorização em questão pode ser uma autorização «única» para proceder de determinada forma com informação pessoal, mas, como ilustram os exemplos seguintes, é provável que seja uma excepção a uma lei mais abrangente que regulamente a recolha, uso e divulgação de informação pessoal.

A lei Telecommunications Act de 1996

Em muitos casos, os usos autorizados são coerentes com as exigências da directiva e dos princípios, ou seriam permitidos por uma das restantes excepções previstas. Por exemplo, a secção 702 da lei Telecommunications Act (codificada em 47 U.S.C. § 222) impõe às empresas de telecomunicações o dever de manter a confidencialidade sobre a informação pessoal que obtêm no decurso dos serviços que efectuam para os seus clientes. Esta disposição permite especificamente às telecomunicações:

1. Usar a informação sobre o cliente para oferecer um serviço, incluindo a publicação de listas de assinantes;

2. Fornecer informação sobre os clientes a terceiros, a pedido dos clientes; e

3. Fornecer informação sobre os clientes de forma agregada.

([12]) Uma pesquisa electrónica recente da base de dados Westlaw mostrou a existência de 994 casos relacionados com a violação da privacidade.

([13]) Para esclarecer, a respectiva autoridade legal não terá que fazer referências específicas ao «porto seguro».

([14]) Da mesma forma, o médico neste exemplo poderá não confiar na autoridade legal para anular a opção de não partricipação da pessoa no marketing directo previsto na FAQ 12. O objectivo de qualquer excepção às «autorizações explícitas» é necessariamente limitado ao âmbito da autorização segundo a respectiva lei.

Ver 47 U.S.C. § 222(c)(1)-(3). A lei abre ainda às empresas de telecomunicações as seguintes excepções para usar informação sobre os clientes:

1. Iniciar, apresentar, facturar e receber pagamento pelos seus serviços;

2. Proteger contra condutas fraudulentas, abusivas ou ilegais; e

3. Fornecer serviços de telemarketing, de arbitragem ou administrativos durante uma chamada iniciada pelo cliente ([15]).

Id., § 222(d)(1)-(3). Finalmente, as empresas de telecomunicações só podem fornecer aos editores de listas telefónicas informações sobre as listas de assinantes que contenham o nome, endereço, número de telefone e ramo de negócio dos clientes comerciais, id., § 222(e).

A excepção de «autorizações explícitas» pode ser invocada quando as empresas de telecomunicações usam CPNI para evitar a fraude ou outro tipo de conduta ilegal. Mesmo nestas condições, essas acções podem qualificar-se de «interesse público» e ser permitidas pelos princípios por essas mesmas razões.

Regras propostas pelo Department of Health and Human Services

O Department of Health and Human Services (HHS) propôs regras em matéria de privacidade de informação identificável sobre a saúde, ver 64 Fed. Reg. 59,918 (3 de Novembro de 1999) (para ser codificado 45 C.F.R. pts. 160-164). As regras implementariam os requisitos da protecção da privacidade previstos pela Health Insurance Portability and Accountability Act de 1996, Pub. L. 104-191. As regras propostas proibiriam em geral as entidades abrangidas (isto é, planos de saúde, câmaras de compensação da segurança social e fornecedores de cuidados de saúde que transmitem informação em formato electrónico) de usar ou divulgar informação confidencial sem consentimento individual, ver proposta 45 C.F.R. § 164.506. Essas mesmas regras exigiram a divulgação de informação confidencial sobre a saúde em dois casos exclusivos: 1) para permitir às pessoas consultar e utilizar as suas próprias informações, ver *id*. em § 164.514; e 2) para aplicar as regras, ver *id*. em § 164.522.

As regras propostas permitiriam usar ou divulgar informação confidencial sobre a saúde, sem autorização específica da pessoa em causa em circunstâncias limitadas, incluindo a supervisão do sistema de saúde, a aplicação da lei e emergências, ver *id*. em § 164.510. As regras propostas definem pormenorizadamente os limites de tais utilizações e divulgações e, ainda, estas seriam limitadas a uma quantidade mínima de informação necessária, ver *id*. em § 164.506.

Os usos permissivos explicitamente autorizados pela regulamentação proposta são geralmente coerentes com os princípios de «porto seguro» ou encontram-se abrangidos por outras excepções, como é o caso da aplicação da lei e da administração judicial ou da investigação médica. Outros usos tais como a supervisão do sistema de saúde, casos de saúde pública, estatísticas oficiais sobre a saúde, são de interesse público. A divulgação de dados para processar pagamentos dos cuidados de saúde e indemnizações é necessária para o funcionamento do próprio sistema de saúde. A utilização nas emergências, para consulta de familiares, nos casos em que o consentimento do paciente «não pode ser prática ou razoavelmente obtido», ou para determinar a identidade ou causa de morte, protegem os interesses vitais das pessoas em questão e outros. A utilização para fins de gestão dos militares no activo e outros grupos particulares de pessoas, contribuem para a execução de missões militares ou outras situações igualmente exigentes; e, em qualquer caso, tais fins terão pouco ou nenhum interesse para o consumidor em geral.

Resta apenas a utilização das informações pessoais pelos sistemas de saúde para produção de listas de doentes. Conquanto tais usos não levantem um problema de interesse «vital», essas listas não beneficiam pacientes, nem amigos ou

([15]) O âmbito desta excepção é muito limitado. Nos seus termos, a empresa de telecomunicações só poderá usar CPNI durante uma chamada iniciada pelo cliente. Além disso, fomos informados pela FCC que a empresa de telecomunicações não pode usar CPNI para comercializar serviços fora dos serviços pedidos pelo cliente. Finalmente, visto que o cliente deve aprovar o uso de CPNI para este fim, esta disposição não é sequer uma «excepção».

relações. O âmbito desta autorização é por inerência limitado. Assim, confiar nas excepções aos princípios para usos «explicitamente autorizados» pela lei para este fim apresenta poucos riscos para a vida privada dos pacientes.

A lei Fair Credit Reporting Act

A Comissão Europeia expressou a preocupação de que as excepções «explicitamente autorizadas» possam «efectivamente criar uma verificação de adequação» por parte de Fair Credit Reporting Act (FCRA). Isto não seria, porém, o caso. Na ausência de uma verificação de adequação específica para a FCRA, as organizações dos EUA que aceitassem tal verificação deveriam aderir aos acordos de «porto seguro» em todos os seus aspectos. Significa isto que quando as exigências da FCRA ultrapassam o nível de protecção assegurado pelos princípios, as organizações norte-americanas apenas terão que obedecer à FCRA. Em contrapartida, quando a FCRA ficar aquém do previsto nos acordos, essas mesmas organizações terão que nivelar as suas práticas de protecção da vida privada pelos princípios de «porto seguro». As excepções não deveriam alterar esta condição básica. Nos seus termos, a excepção aplica-se apenas aos casos em que a lei em questão autorize explicitamente condutas incoerentes com os princípios de «porto seguro». A excepção não abrangeria os casos em que os requisitos da FCRA não estejam ao nível dos princípios de «porto seguro» ([16]).

Por outras palavras, não pretendemos que a excepção signifique que o que não se encontra estipulado possa ser assim considerado «explicitamente autorizado». Mais, a excepção aplica-se apenas quando o que é permitido pela lei dos EUA contradiz as exigências dos princípios de «porto seguro». A lei em questão deve responder a ambos os requisitos antes da não adesão aos princípios ser permitida.

A secção 604 da FCRA, por exemplo, autoriza explicitamente as agências de informações comerciais a emitir relatórios sobre os consumidores em vários casos concretos, ver FCRA, § 604. Se, ao fazê-lo, a secção 604 autorizasse as agências de informações comerciais a agir em detrimento dos princípios do «porto seguro», então estas teriam que recorrer às excepções (a não ser que surja outra). Estas agências de informações comerciais devem acatar as ordens do tribunal e as sanções do júri, e a utilização de informações comerciais por parte das agências autorizadas, das entidades públicas e das instituições de apoio à criança tem uma finalidade de interesse público, *id.*, § 604(a)(1), (3)(D), e (4). Consequentemente, as agências de informações comerciais não necessitariam de confiar nas excepções das «autorizações explícitas» para tal. Quando actua em conformidade com instruções escritas do consumidor, a agência de informações está em perfeita sintonia com os princípios do «porto seguro», *id.*, § 604(a)(2). Da mesma forma, os relatórios sobre o consumidor só podem ser obtidos para fins laborais com o consentimento escrito do consumidor [*id.*, §§ 604(a)(3)(B) e (b)(2)(A)(ii)] e para transacções comerciais ou de seguros que não sejam iniciadas pelo consumidor se este não tiver escolhido tais exigências [*id.*, § 604(c)(1)(B)]. Ademais, a FCRA proíbe as agências de informações comerciais de divulgar informações médicas para fins laborais sem o consentimento do consumidor, *id.*, § 604(g). Tais usos são compatíveis com os princípios de aviso e escolha. Outros fins autorizados pela secção 604 dizem respeito a transações envolvendo o consumidor e seriam permitidas pelos princípios por essa razão, ver *id.*, § 604(a)(3)(A) e (F).

Os restantes usos «autorizados» pela secção 604 dizem respeito a mercados secundários, *id.*, § 604(a)(3)(E). Não existe conflito entre o uso de informação sobre o consumidor para este fim e os princípios de «porto seguro» em si. É verdade que a FCRA não exige das agências de informação comercial que avisem e peçam consentimento do consumidor quando divulgam informação para este fim. Contudo, reiteramos o facto de que a ausência de um requisito não pode ser conotada com uma «autorização explícita» para agir de maneira incompatível com as normas. Da mesma forma, a secção 608 permite às agências de informação comerciais que divulguem informação pessoal às entidades governamentais. Esta «autorização» não justifica que a agência ignore o seu compromisso de adesão aos princípios de «porto seguro». Isto contrasta com outros exemplos nossos onde as excepções ao princípio de aviso e de escolha funcionam de forma a autorizar explicitamente a utilização de informação pessoal sem aviso e escolha.

Conclusão

Da nossa análise sucinta destas normas destaca-se um padrão distinto:

— a «autorização explícita» prevista na lei geralmente permite o uso ou a divulgação de informação pessoal sem o consentimento prévio da pessoa em causa; assim, a excepção seria limitada aos princípios de aviso e de escolha,

([16]) As nossas conversações neste aspecto não devem fazer pensar que consideramos que a FCRA não proporciona protecção «adequada». Qualquer avaliação da FCRA deve ter em conta a protecção fornecida pela lei na sua totalidade e não focar apenas as excepções como fazemos aqui.

— na maior parte dos casos, as excepções autorizadas pela lei são limitadas a situações e fins específicos. De outra forma, a lei proíbe sempre a utilização sem autorização ou a divulgação de informação pessoal que não se encontra abrangida por estas situações e fins,

— na maior parte dos casos, devido ao seu carácter legal, a utilização ou divulgação autorizadas servem o interesse público,

— em quase todos os casos, as utilizações autorizadas são perfeitamente coerentes com os princípios de «porto seguro» ou com as excepções permitidas.

Para concluir, o âmbito das excepções por «autorizações explícitas» previstas na lei será, pelo seu próprio carácter, bastante limitado.

C. **Fusões e Aquisições**

O grupo de trabalho do artigo 29.º manifestou alguma preocupação relativamente a situações em que a organização aderente ao «porto seguro» é objecto de aquisição ou fusão e a segunda organização não pertence ao «porto seguro». O grupo de trabalho, contudo, parece ter considerado que nada obriga a entidade resultante da operação a aplicar os princípios de «porto seguro» às informações detidas pela primeira organização, mas o direito norte-americano em nada obriga a que assim seja. A regulamentação dos EUA sobre fusões e aquisições estipula que uma empresa que adquire outra assume as obrigações e responsabilidades da primeira, ver 15 Flechter Cyclopedia of the Law of Private Corporations § 7117 (1990); ver ainda Model Bus. Corp. Act § 11.06(3) (1979) («a companhia resultante assume todas as obrigações das diferentes partes envolvidas na fusão»). Por outras palavras, a companhia resultante de uma fusão de uma organização participante no «porto seguro» por este método estará sujeita aos compromissos assumidos pela outra, em termos de «porto seguro».

Além do mais, mesmo que a fusão seja efectuada através da aquisição de activos, as responsabilidades da empresa podem apesar disso passar para a compradora em certas circunstâncias, 15 Flechter, § 7122. Mesmo nos casos em que a responsabilidade civil não se mantenha com a fusão, vale a pena notar que esta nunca sobreviveria a uma fusão em que os dados fossem transferidos a partir da Europa nos termos de um contrato — a única alternativa viável ao «porto seguro» para a transferência de dados para os EUA. Além disso, os documentos do «porto seguro» tal como agora revistos exigem que todas as organizações aderentes notifiquem o Department of Commerce de qualquer aquisição para que a continuação da transferência dos dados para o sucessor da primeira organização só seja possível se também este pertencer ao «porto seguro», ver FAQ 6. De facto, os EUA reviram o enquadramento do «porto seguro» para exigir às organizações dos EUA nesta situação que eliminem informação recebida ao abrigo dos acordos se a sua adesão aos acordos não se mantiver ou se não forem aplicadas outras cláusulas de salvaguarda adequadas.

ANEXO V

14 de Julho de 2000

John Mogg
Director-Geral, DG Mercado Interno
Comissão Europeia
C 107-6/72
Rue de la Loi/Wetstraat 200
B-1049 Bruxelas

Excelentíssimo Senhor,

Tomei conhecimento de que a minha carta de 29 de Março de 2000 suscitou uma série de questões. A fim de clarificar a competência dos nossos serviços nas áreas em que essas questões se colocam, envio a presente carta, que, para facilitar futuras referências, complementa e recapitula em parte o teor da correspondência precedente.

Nas visitas efectuadas aos nossos serviços e na vossa correspondência, foram colocadas várias questões relativas à jurisdição da Federal Trade Commission dos Estados Unidos sobre protecção da vida privada na área das comunicações em linha. Julguei ser útil resumir as minhas respostas anteriores e fornecer informações adicionais sobre a jurisdição deste organismo quanto às questões relacionadas com a vida privada do consumidor colocadas na vossa última carta. Em particular, as vossas perguntas incidiam sobre o seguinte: 1. Se a FTC tem competência no domínio das transmissões de dados relacionados com o emprego, sempre que estas violem os princípios de «porto seguro» dos Estados Unidos; 2. Se a FTC tem competência em matéria de programas homologados («seal») de carácter não lucrativo; 3. Se o FTC Act se aplica não só ao sector em linha, mas também ao fora de linha; e 4. O que acontece quando se verifica uma sobreposição entre as competências da FTC e as de outros organismos também responsáveis pela aplicação da lei.

FTC Act: aplicação à protecção da vida privada

A jurisdição da Federal Trade Commission encontra-se definida no artigo 5.º (Section 5) da lei Federal Trade Commission Act, que proíbe «os actos ou as práticas desleais ou enganosas» no âmbito da actividade comercial ou que sobre esta incidam [1]. Uma prática enganosa é definida como uma representação, omissão ou prática susceptível de induzir em erro um consumidor razoável. Uma prática é desleal se causa, ou é susceptível de causar, danos substanciais aos consumidores que não possam ser facilmente evitados e não sejam contrabalançados por benefícios compensatórios para os consumidores ou para a concorrência [2].

Determinadas práticas de recolha de informação tendem a violar as disposições do FTC Act. Por exemplo, se um sítio da internet declarar falsamente que obedece à política de protecção da vida privada ou a um conjunto de directrizes auto-regulamentadoras, o artigo 5.º do FTC Act constitui uma base jurídica que permite contestar essas falsas afirmações como enganosas. Com efeito, a aplicação bem sucedida da lei permitiu o estabelecimento deste princípio [3]. Além disso, a FTC adoptou a posição de poder vir a acusar de práticas desleais práticas de protecção da vida privada particularmente flagrantes, nos termos do artigo 5.º, se envolverem crianças, ou fizerem uso de informação particularmente sensível, como relatórios financeiros [4] e relatórios médicos. A Federal Trade Commission tem adoptado e continuará a adoptar tais medidas de aplicação da lei, com base no seu esforço de supervisão e de investigação e em queixas recebidas de organizações auto-regulamentadoras e outras, incluindo dos Estados-Membros da União Europeia.

---

[1] 15 U.S.C § 45. O Fair Credit Rporting Act também se aplicaria a recolhas de dados e vendas via internet que se enquadrem nas definições legais de «relatórios sobre os consumidores» e «gabinetes de estudos de mercado».

[2] 15 U.S.C. § 45(n).

[3] Ver GeoCities, Docket n.º C-3849 (decisão transitada em julgado em 12 de Fevereiro de 1999) disponível em www.ftc.gov/os/ /1999/9902/9823015d%26o.htm); Liberty Financial Cos., Docket n.º C-3891 (decisão transitada em julgado em 12 de Agosto de 1999) (disponível em www.ftc.gov/opa/1999/9905/younginvestor.htm), ver também Children's Online Privacy Protection Act Rule (COPPA), 16 C.F.R. Parte 312 (disponível em www.ftc.gov/opa/1999/9910/childfinal.htm). A COPPA Rule, que entrou em vigor no mês passado, requer que os operadores de sítios na internet dirigidos a crianças com menos de 13 anos de idade, ou que reconhecidamente recolham dados pessoais de crianças dessas idades, apliquem os códigos de boas práticas de informação enunciados neste diploma.

[4] Ver FTC v. Touch Tone, Inc., Civil Action n.º 99-WM-783 (D.Co.) (de 21 de Abril de 1999) em ⟨www.ftc.gov/opa/1999/9904/touchtone.htm⟩. Staff Opinion Letter, 17 de Julho de 1997, emitida em resposta a uma petição arquivada pelo Center of Media Education, em ⟨www.ftc.gov/os/1997/9707/cenmed.htm⟩.

Apoio à auto-regulamentação

A FTC dará prioridade a queixas por incumprimento de directrizes auto-regulamentadoras recebidas de organizações tais como BBBOnline e TRUSTe ([5]). Esta abordagem seria coerente com a nossa relação duradoura com o National Advertising Review Board (NARB), do Better Business Bureau, que remete queixas relativas à publicidade para a FTC. A National Advertising Division (NAD), do NARB, recorre ao processo judicial para resolver queixas relativas a publicidade nacional. Quando uma das partes recusa cumprir uma decisão da NAD, é apresentada queixa à FTC. Os funcionários da FTC reexaminam prioritariamente a publicidade contestada para determinar se esta viola o FTC Act e, frequentemente, conseguem pôr cobro à prática contestada ou persuadir a parte em causa a regressar ao processo NARB.

Do mesmo modo, a FTC dará prioridade a quexas por incumprimento baseadas nos princípios de «porto seguro» e oriundas dos Estados-Membros. Tal como acontece com queixas provenientes das organizações auto-regulamentadoras dos EUA, os nossos funcionários apreciarão qualquer informação recebida procurando determinar se a prática contestada infringe as disposições do artigo 5.º do FTC Act. Este compromisso também pode ser encontrado nos princípios de «porto seguro» incluídos nas questões mais frequentes (FAQ 11) sobre aplicação.

GeoCities: o primeiro caso da FTC relativo à protecção da vida privada na internet

O primeiro caso da Federal Trade Commission relativo à protecção da vida privada no domínio da internet, GeoCities, baseava-se na autoridade da FTC em aplicação do artigo 5.º ([6]). Neste caso, a FTC alegou que a GeoCities veiculara falsas informações, quer a adultos quer a crianças, quanto à forma como os respectivos dados pessoais seriam utilizados. A queixa apresentada pela Federal Trade Commission alegava que a GeoCities declarava que as informações de identificação pessoal recolhidas no seu sítio da internet seriam apenas utilizadas para fins internos ou para fornecer aos consumidores ofertas publicitárias específicas e produtos ou serviços por eles solicitados, e que determinadas informações suplementares «facultativas» não seriam transmitidas a ninguém sem a autorização do consumidor. Na realidade, este tipo de dados foi facultado a terceiros, que os utilizaram para solicitar os clientes excedendo em muito o que tinha sido acordado. A queixa também acusava a GeoCities de estar envolvida em práticas enganosas relacionadas com a recolha de dados relativos a crianças. De acordo com a queixa da FTC, a GeoCities afirmava ter uma página dirigida às crianças no seu sítio da internet e que a informação nele recolhida era gerida pela GeoCities. Na verdade, esses sectores do seu sítio internet eram geridos por terceiros, que recolhiam e tratavam a informação.

A decisão judicial proíbe a GeoCities de prestar falsas declarações quanto ao fim para que são recolhidos os dados pessoais dos consumidores ou sobre os consumidores, incluindo os de crianças. Exige que a empresa coloque no seu sítio da internet um aviso claro e bem visível sobre a sua política de protecção da vida privada, indicando aos consumidores que informação está ser recolhida e com que objectivo, a quem será transmitida e de que modo podem os consumidores aceder a essa informação e eliminá-la. Para assegurar a possibilidade de controlo parental, esta decisão também requer que a GeoCities obtenha essa autorização antes de recolher dados pessoais de crianças com idade igual ou inferior a 12 anos. Nos termos da decisão, a GeoCities deve informar os seus membros e dar-lhes a possibilidade de eliminar a respectiva informação das bases de dados da GeoCities e de qualquer uma das bases de dados de terceiros envolvidos. A decisão requer especificamente que a GeoCities informe os pais de crianças com idade igual ou inferior a 12 anos e que elimine os dados a estas relativos, a não ser que um dos pais consinta explicitamente na sua preservação e utilização. Por último, a GeoCities deve também contactar os terceiros envolvidos, a quem transmitiu previamente estes dados, solicitando-lhes que eliminem também essa informação das suas bases de dados ([7]).

ReverseAuction.com

Em Janeiro de 2000, a FTC aceitou uma queixa contra um sítio de leilões na internet, a ReverseAuction.com, com a qual celebrou subsequentemente um acordo e que alegadamente obtinha dados pessoais dos consumidores a partir de um sítio pertencente à concorrência (eBay.com) e enviava posteriormente mensagens electrónicas não solicitadas e enganosas aos consumidores que procuravam os serviços desta última empresa ([8]). A queixa que apresentámos alega que a ReverseAuction violou o artigo 5.º da FTC Act, ao obter dados pessoais identificáveis, que incluíam os endereços de correio electrónico e os números de identificação pessoal dos utilizadores da eBay, bem como ao enviar as mensagens enganosas.

([5]) De facto, a FTC apresentou recentemente uma queixa ao Federal District Court contra um utilizador da homologação («sealholder») TRUSTe, Toysmart.com, para obter medidas cautelares e declarativas a fim de impedir a venda de dados pessoais e confidenciais dos clientes recolhidos no sítio internet da empresa, infringindo a sua própria política de protecção da vida privada. A FTC foi informada desta eventual violação da lei directamente pela TRUSTe, FTC v. Toysmart.com, LLC, Civil Action n.º 00-11341-RGS (D.Ma.) (apresentado em 11 de Julho de 2000) (disponível em www.ftc.gov/opa/2000/07/toysmart.htm).

([6]) GeoCities, Docket n.º C-3849 (decisão já transitada em julgado em 12 de Fevereiro de 1999) disponível em www.ftc.gov/os/ /1999/9902/9823015d%26o.htm).

([7]) A FTC decidiu também um outro caso relacionado com a recolha de dados de crianças na internet. A Liberty Financial Companies, Inc., operava o sítio Young Investor na internet dirigido a crianças e adolescentes, concentrando a sua actividade em questões relacionadas com dinheiro e investimentos. A FTC alegou que, nesse endereço, se afirmava falsamente que os dados pessoais dos jovens, recolhidos através de um inquérito, seriam mantidos no anonimato e que uma publicação electrónica e prémios seriam enviados aos participantes. Na realidade, os dados pessoais recolhidos sobre a situação financeira dos jovens e das suas famílias eram mantidos de forma bem identificável e não lhes foram enviados quaisquer publicações ou prémios. O acordo proíbe futuras declarações fraudulentas e exige que a Liberty Financial coloque nos seus sítios da internet dirigidos às crianças um aviso relativo à sua política de protecção da vida privada e obtenha a autorização comprovada dos pais, antes de recolher dados pessoais junto de crianças. Liberty Financial Cos., Docket n.ºC-3891 (decisão já transitada em julgado em 12 de Agosto de 1992) (disponível em www.ftc.gov/opa/ /1999/9905/younginvestor.htm).

([8]) Ver ReverseAuction.com, Inc., Civil Action n.º 000032 (D.D.C.) (apresentado em 6 de Janeiro de 2000) (comunicado à imprensa e alegações em www.ftc.gov/opa/2000/01/reverse4.htm).

Tal como se indicava na queixa, antes de obter a informação, a ReverseAuction inscreveu-se como utilizadora da eBay e comprometeu-se a respeitar os termos de utilização propostos pela eBay e a sua política de protecção da vida privada. Os termos de utilização e a política adoptados protegem a vida privada dos consumidores, proibindo os utilizadores da eBay de utilizar e recolher dados pessoais para fins não autorizados, tais como o envio de mensagens electrónicas não solicitadas. Assim, a queixa por nós interposta alegava que a ReverseAuction fizera falsas declarações de cumprimento dos termos de utilização e da política da eBay, uma prática enganosa nos termos do artigo 5.º Em alternativa, a queixa alegava que a utilização da informação por parte da ReverseAuction para enviar as mensagens electrónicas enganosas, infringindo os termos de utilização e a política de protecção da vida privada da eBay, era considerada uma prática fraudulenta, em conformidade com o mesmo artigo 5.º

Em segundo lugar, a queixa alegava que as mensagens enviadas aos consumidores por correio electrónico continham uma referência enganosa, «informando-os» de que o seu número de identificação pessoal de utilizador da eBay «expirava em breve». Por último, a queixa alegava que as mensagens electrónicas indicavam falsamente que a eBay fornecia, directa ou indirectamente, os dados pessoais dos utilizadores à ReverseAuction, ou participava de algum modo na difusão das referidas mensagens electrónicas.

A decisão obtida pela FTC proíbe a ReverseAuction de cometer tais violações no futuro. Exige também à ReverseAuction que informe os consumidores que, na sequência da recepção da sua mensagem, pretendiam inscrever-se como clientes da ReverseAuction de que os seus números de identificação pessoal como utilizadores da eBay não iriam deixar de ser válidos e que esta empresa não tivera conhecimento, nem autorizara, a difusão dessa mensagem electrónica por parte da ReverseAuction. Esta informação permitiria também aos consumidores cancelar a sua inscrição junto da ReverseAuction e solicitar que a ReverseAuction eliminasse os seus dados de identificação pessoal da respectiva base de dados. Além disso, a decisão exige que a ReverseAuction elimine, e se abstenha de usar ou revelar, os dados de identificação pessoal dos membros da eBay que receberam a mensagem da ReverseAuction, mas que não se inscreveram junto desta empresa. Por último, em consonância com outras decisões na matéria obtidas por este organismo, a decisão exige que a ReverseAuction revele, no seu sítio da internet, a política por ela adoptada em termos de protecção da vida privada e inclui uma extensa lista de disposições sobre registo de dados que permitem à FTC supervisionar o cumprimento destas exigências.

O caso da ReverseAuction demonstra que a FTC está empenhada em aplicar a lei para apoiar os esforços de auto-regulamentação da indústria no domínio da protecção da vida privada dos consumidores em linha. Com efeito, este caso contestava directamente uma prática perniciosa em relação a uma política empresarial de protecção da vida privada e a um acordo de termos de utilização com os utilizadores e que poderia destruir também a confiança dos consumidores em medidas de protecção da vida privada adoptadas por empresas em linha. Por se tratar de um caso de apropriação indevida por parte de uma empresa dos dados de consumidores protegidos por uma outra empresa, este exemplo assume também particular relevância relativamente às preocupações de protecção da vida privada suscitadas pela transmissão de dados entre empresas de países diferentes.

Não obstante as medidas para aplicação da lei adoptadas pela Federal Trade Commission nos casos da GeoCities, Liberty Financial Cos. e ReverseAuction, a jurisdição deste organismo em algumas áreas de protecção dos dados pessoais em linha é mais limitada. Tal como já antes se disse, para poder ser abrangida pelo FTC Act, a recolha e utilização de dados pessoais sem consentimento tem de constituir uma prática comercial, quer enganosa, quer desleal. Assim, o FTC Act não seria provavelmente aplicável às práticas realizadas num sítio da internet em que sejam recolhidos dados pessoais dos consumidores, mas em que não se apresentem falsas declarações acerca do propósito desta mesma recolha, ou que não implique a transmissão dessa informação de formas que possam causar danos substanciais aos consumidores. Do mesmo modo, poderá não estar actualmente no poder da FTC exigir, em regra, que as entidades que se dedicam à recolha de dados na internet adoptem uma política de protecção da vida privada ou adiram a qualquer destas políticas já existentes ([9]). Como acima se disse, contudo, o incumprimento por parte de uma empresa da política de protecção da vida privada por si declarada pode ser considerada uma prática enganosa.

([9]) Por esta reazão a Federal Trade Commission declarou ao Congresso que seria provavelmente necessária legislação adicional para decretar que todos os sítios comerciais dos EUA na internet dirigidos aos consumidores cumprissem práticas específicas e leais de informação «Consumer Privacy on the World Wide Web», Before the Subcommittee on Telecommunications, Trade and Consumer Protection of the House Committee on Commerce United States House of Representatives, 21 de Julho de 1998 (a declaração pode ser consultada em www.ftc.gov/os/9807/privac98.htm). A FTC adiou o pedido de tal legislação para dar aos esforços auto-regulamentadores a oportunidade de demonstrar a adopção generalizada de práticas leais de informação nos sítios da internet. No relatório da Federal Trade Commission ao Congresso sobre a protecção da vida privada, «Privacy Online: A Report to Congress», Junho de 1998 (o relatório pode ser encontrado em www.ftc.gov/reports/privacy3/toc.htm), a FTC recomendou legislação exigindo que os sítios comerciais na internet obtivessem o consentimento prévio por parte da entidade parental, antes de recolherem dados pessoais de crianças e jovens com idades inferiores a 13 anos, ver nota de rodapé n.º 3 *supra*. No ano passado, o relatório da FTC, «Self-Regulation and Privacy Online: A Federal Trade Commission Report to Congrtess», Julho de 1999 (pode ser consultado em www.ftc.gov/os/ /1999/9907/index.htm#13), concluiu que tinha havido progressos consideráveis no domínio da auto-regulamentação e, consequentemtente, optou por não recomendar a adopção de legislação nessa altura.
Em Maio de 2000, a FTC apresentou um terceiro relatório ao Congresso, «Privacy Online: Fair Information Practices in the Electronic Marketplace» (o relatório pode ser consultado em www.ftc.gov/os/2000/05/index.htm#22), que debate o estudo realizado recentemente pela FTC sobre sítios comerciais na Internet e a sua observância das práticas leais de informação. O relatório também recomendava (por maioria da FTC) que o Congresso aprovasse legislação que estabelecesse um nível mínimo de protecção da vida privada para os sítios comerciais da internet dirigidos aos consumidores.

Além disso, a competência da FTC nesta matéria só abrange actos ou práticas desleais ou enganosos se estes «forem de carácter comercial ou afectarem a actividade comercial». A recolha de informação por parte de entidades comerciais que promovam produtos ou serviços, inclusive a recolha e utilização da informação para fins comerciais, satisfaria presumivelmente o requisito «comercial». Por outro lado, muitos indivíduos ou entidades podem estar a efectuar recolhas de dados em linha sem qualquer propósito comercial, estando, por isso, fora da alçada da Federal Trade Commission. Um exemplo de tais limitações envolve os «chat rooms» («grupos de discussão») quando geridos por entidades não comerciais, como uma instituição de caridade, por exemplo.

Por último, a competência fundamental da FTC relativamente às práticas comerciais conta com um certo número de exclusões, totais ou parciais, que restringem a capacidade da FTC de fornecer uma resposta abrangente às preocupações de protecção da vida privada na internet. Tais exclusões abrangem muitas empresas que tratam intensivamente a informação dos consumidores, tais como bancos, companhias de seguros e companhias aéreas. Como devem saber, outros serviços federais e estatais são competentes relativamente a estas entidades, tais como os serviços bancários federais ou o Department of Transportation.

No casos que são da sua competência, a FTC aceita e, se os recursos o permitirem, actua em caso de queixas apresentadas por consumidores e recebidas por correio electrónico e telefone no seu Consumer Reponse Center (CRC) e, mais recentemente, no seu sítio da internet ([10]). O CRC aceita queixas de todos os consumidores, incluindo dos residentes nos Estados-Membros da União Europeia. O FTC Act atribui à Federal Trade Commission poderes equitativos para proferir injunções contra futuras violações do FTC Act, bem como para obtenção de reparações dos danos causados aos consumidores. Teríamos, contudo, o cuidado de verificar se a empresa se teria envolvido num padrão de conduta impróprio, dado que não resolvemos litígios individuais de consumo. No passado, a Federal Trade Commission proporcionou reparações a cidadãos quer dos Estados Unidos, quer de outros países ([11]). A FTC continuará a afirmar a sua autoridade, nos casos apropriados, de modo a providenciar reparações para os cidadãos de outros países que sofreram danos por práticas enganosas que recaem sob a sua jurisdição.

Dados sobre o Emprego

A vossa última carta procurava obter esclarecimentos adicionais relativos à competência da FTC em matéria de dados sobre o emprego. Em primeiro lugar, foi colocada a questão de saber se a FTC poderia actuar, ao abrigo do artigo 5.º, contra uma empresa que declara cumprir os princípios de «porto seguro» dos EUA, mas transfere ou utiliza dados relacionados com o emprego de um modo tal que infringe estes princípios. Gostaríamos de vos assegurar que procedemos a uma revisão cuidada da legislação da FTC que autoriza tais operações, dos documentos correlacionados e da jurisprudência relevante e concluímos que a FTC possui, sobre os dados relacionados com o emprego, a mesma competência que teria em geral nos termos do artigo 5.º da FTC Act ([12]). O mesmo é dizer que poderíamos também actuar numa situação relativa a dados sobre o emprego, assumindo que um caso corresponde aos nossos critérios (deslealdade ou carácter enganoso) de adopção de medidas para aplicação da lei no domínio da protecção da vida privada.

Gostaríamos também de alterar qualquer ideia errónea de que a capacidade de a FTC adoptar medidas para aplicação da lei relacionadas com a protecção da vida privada se limita às situações em que uma empresa ludibriou consumidores individuais. Com efeito, tal como o processo da FTC contra a ReverseAuction ([13]) torna claro, a FTC adoptará medidas para aplicação da lei em matéria de protecção da vida privada em situações que envolvem transferências de dados entre empresas, em que uma empresa alegadamente agiu de forma ilegal face a outra empresa, conduzindo eventualmente a danos causados a empresas e consumidores. Cremos que este será o tipo de situação em que as questões relacionadas com o emprego tenderão mais facilmente a surgir, dado que os dados sobre emprego são transferidos de empresas europeias para empresas americanas, que se comprometeram a respeitar os princípios de «porto seguro».

No entanto, gostaríamos de sublinhar uma circunstância em que a actuação da FTC seria circunscrita. Trata-se de situações em que a questão apresentada já está a ser resolvida no âmbito do contexto jurídico tradicional do direito do trabalho, muito provavelmente através de uma reclamação ou de um pedido de arbitragem, ou de uma queixa apresentada ao National Labor Relations Board por práticas fraudulentas a nível laboral. Isto sucederia, por exemplo, se, no âmbito

([10]) Ver http://www.ftc.gov/ftc/complaint.htm relativamente ao formulário electrónico para apresentação de queixa da Federal Trade Commission.

([11]) Por exemplo, num caso recente, que envolvia um sistema de vendas em pirâmide na internet, a FTC obteve reembolsos para 15 622 consumidores, totalizando, aproximadamente, 5,5 milhões USD. Os referidos consumidores eram residentes nos EUA e em 70 países estrangeiros, ver www.ftc.gov/opa/9807/fortunar.htm; www.ftc.gov/opa/9807/ftcrefund01.htm.

([12]) Excepto se excluído especificamente pelo estatuto da FTC, a jurisdição da FTC, nos termos do FTC Act, sobre práticas «no âmbito da actividade comercial ou que sobre esta incidam», é idêntica ao poder contituicional do Congresso ao abrigo da Commerce Clause, United States v. American Building Maintenance Industries, 422 U.S. 271, 277 n. 6 (1975). A jurisdição da FTC abrangeria, pois, práticas relacionadas com o emprego em empresas e indústrias do comércio internacional.

([13]) Ver «Online Auction Site Settles FTC Privacy Charges», FTC News Release (6 de Janeiro de 2000), disponível em http://www.ftc.gov/opa/2000/01/reverse4.htm.

de um acordo colectivo relativo à utilização de dados pessoais, um empregador tivesse assumido um compromisso e um empregado ou sindicato alegassem que a entidade patronal tinha quebrado esse acordo. A FTC não interviria provavelmente num processo deste tipo ([14]).

Competência em matéria de programas homologados («seal»)

Em segundo lugar, é-nos colocada a questão de saber se a jurisdição da FTC seria extensiva a programas homologados («seal») e que gerem mecanismos de resolução de litígios nos Estados Unidos, sempre que estes tenham exercido abusivamente o seu papel, ao aplicarem princípios de «porto seguro» e ao lidarem com queixas individuais — ainda que tais entidades sejam, tecnicamente, declaradas «não lucrativas». Ao determinar se uma entidade que se designa a si própria como não lucrativa recai sob a sua jurisdição, a FTC analisa cuidadosamente se essa entidade, embora não procurando obter lucros em proveito próprio, promove ou não o lucro para os seus membros. A FTC conseguiu impor a sua autoridade sobre essas entidades e, muito recentemente, em 24 de Maio de 1999, o Supremo Tribunal dos Estados Unidos, no processo intitulado California Dental Association v. Federal Trade Commission, declarou unanimemente a competência da FTC relativamente a uma associação voluntária e não lucrativa de empresas locais de medicina dentária no âmbito de um caso de defesa da concorrência. O Tribunal considerou que:

> O FTC Act procura, com dificuldade, abranger não só entidades «organizadas para realizar negócios com fins lucrativos», 15 U.S. C. § 44, mas também as que realizam negócios em benefício «dos seus membros» … Seria difícil supor, de facto, que o Congresso pretendesse uma definição tão restrita das organizações de apoio abrangidas, tendo em vista as oportunidades que tal proporcionaria de escapar à sua autoridade, quando os objectivos do FTC Act requerem obviamente a confirmação dessa mesma autoridade.

Em suma, determinar se é possível exercer as nossas competências em relação a uma entidade particular de carácter «não lucrativo» e que administre um programa homologado («seal») exigiria uma análise no sentido de determinar em que medida essa entidade proporciona benefícios económicos aos seus membros. Se tal entidade operar o seu programa homologado («seal») de tal modo que este produza benefícios económicos para os respectivos membros, a FTC exercerá, muito provavelmente, a sua autoridade. É de notar que um programa homologado GeoCities fraudulento que forje um estatuto de entidade não lucrativa recairia provavelmente sob a alçada da FTC.

Protecção da vida privada no sector fora de linha

Em terceiro lugar, é necessário sublinhar que a nossa correspondência prévia se centrou na questão da protecção da vida privada no sector em linha. Embora a protecção da vida privada em linha tenha constituído uma preocupação fundamental da FTC, enquanto componente crítica do comércio electrónico, o FTC Act remonta a 1914 e aplica-se igualmente aos sectores tradicionais. Assim, pdemos processar empresas fora de linha que se envolvam em práticas comerciais desleais ou enganosas relacionadas com a vida privada dos consumidores ([15]). Com efeito, num caso apresentado pela FTC no ano passado, FTC v. TouchTone Information, Inc., ([16]) um prospector e vendedor de informações de carácter comercial foi acusado de obter e vender ilegalmente dados financeiros de carácter privado dos consumidores. A FTC alegou que a Touch Tone obteve informações dos consumidores através de «pretexting», expressão criada por uma empresa de investigação privada para descrever a prática de obter dados pessoais sobre outrem usando falsos pretextos, tradicionalmente por telefone. O caso, apresentado em 21 de Abril de 1999, no Tribunal Federal do Colorado, reclama uma injunção e o reembolso de todos os lucros obtidos ilegalmente.

Esta experiência de aplicação da lei, bem como preocupações recentes sobre a fusão de bases de dados em linha e fora de linha, o esbater da distinção entre comércio electrónico e não electrónico e o facto de uma grande quantidade de dados pessoais ser recolhida e utilizada fora de linha tornam claro que está a ser concedida uma atenção significativa a questões relacionadas com a protecção da vida privada no sector não electrónico.

Sobreposição de jurisdições

Por último, coloca-se a questão da interligação da jurisdição da FTC com a de outros serviços federais que garantem a aplicação da lei, particularmente nos casos em que essas jurisdições se sobrepõem. Temos vindo a desenvolver sólidas

([14]) A questão de determinar se uma conduta constitui uma «prática laboral fraudulenta» ou uma violação de um acordo colectivo é uma questão técnica, que é normalmente reservada aos tribunais especializados em direito do trabalho, competentes para apreciar as queixas, às instâncias de arbitragem e ao NRLB.

([15]) Como devem saber, com base em discussões anteriores, o Fair Credit Reporting Act também atribui à FTC competência para proteger a privacidade financeira dos consumidores, ao abrigo do Act, e a FTC emitiu recentemente uma decisão sobre este assunto, ver In the Matter of Trans Union, Docket n.º 9255 (1 de Março de 2000) (comunicado à imprensa e parecer disponíveis em www.ftc.gov/os/2000/03/index.htm#1).

([16]) Civil Action 99-WM-783 (D.Colo.) (disponível em http://www.ftc.gov/opa/1999/9904/touchtone.htm) (está pendente uma decisão relativa a uma tentativa de acordo).

relações de trabalho com numerosos outros organismos desta natureza, incluindo os serviços bancários federais e os procuradores-gerais estaduais. É frequente coordenarmos investigações para maximizar os nossos recursos em instâncias cujas jurisdições se sobrepõem. É também frequente remetermos assuntos para o serviço federal ou estadual de investigação.

Na expectativa de que esta revisão vos seja útil, permaneço à vossa disposição para futuros contactos, caso necessitem de informações complementares.

Com os melhores cumprimentos,

Robert Pitofsky

ANEXO VI

Ex.mo Sr. John Mogg
Director-Geral da DG XV
Comissão Europeia
C 107-6/72
Rue de la Loi/Wetstraat 200
B-1049 Bruxelas

Excelentíssimo Senhor Director-Geral,

Envio esta carta a Vossa Excelência a pedido do Department of Commerce dos EUA, a fim de explicar o papel do Department of Transportation na protecção da privacidade dos consumidores relativamente às informações por estes facultadas às companhias de transportes aéreos.

O Department of Transportation incentiva a auto-regulação, na medida em que a considera o meio menos abusivo e mais eficaz de assegurar a privacidade das informações prestadas pelos consumidores às companhias de transportes aéreos e, desse modo, apoia a criação de um regime de «porto seguro» que permita a essas companhias cumprirem os requisitos da directiva da União Europeia relativa à privacidade, no que toca às tranferências e dados para fora da União Europeia. O Department reconhece, porém, que, para os esforços de auto-regulação funcionarem, é essencial que as companhias aéreas que se tenham comprometido a cumprir os princípios de privacidade definidos no regime de «porto seguro» os cumpram de facto. A este respeito, a auto-regulação deve ser apoiada pela execução legal. Por isso, recorrendo à competência jurídica de que dispõe para a protecção dos consumidores, o Department assegurará o cumprimento dos compromissos de privacidade das companhias aéreas, assumidos para com o público, e instruirá processos por alegada não conformidade na sequência de queixas que receba de organizações de auto-regulação e de outras organizações, inclusive dos Estados-Membros da União Europeia.

A autoridade do Department para tomar medidas de execução neste domínio encontra-se no título 49, secção 41712, do U.S.C., que proíbe uma transportadora aérea de adoptar «práticas desleais ou enganosas e métodos desleais de concorrência» na venda de passagens aéreas, práticas essas que sejam ou possam ser prejudiciais para o consumidor. A secção 41712 segue o modelo da secção 5 do Federal Trade Commission Act (título 15, secção 45, do U.S.C.). Contudo, as companhias de transportes aéreos estão isentas do regulamento da secção 5 pela Federal Trade Commission, ao abrigo do título 15, secção 45(a)(2), do U.S.C.

O serviço a que pertenço investiga e instrui os casos que se enquadram no título 49, secção 41712, do U.S.C. (ver, por exemplo, DOT Orders 99-11-5 de 9 de Novembro de 1999; 99-8-23 de 26 de Agosto de 1999; 99-6-1 de 1 de Junho de 1999; 98-6-24 de 22 de Junho de 1998; 98-6-21 de 19 de Junho de 1998; 98-5-31 de 22 de Maio de 1998; 97-12-23 de 18 de Dezembro de 1997.) Instruímos estes casos com base nas nossas próprias investigações, assim como em queixas formais ou informais apresentadas por pessoas, agentes de viagens, companhias aéreas e entidades estatais norte-americanas ou estrangeiras.

Gostaria de frisar que o facto de uma companhia aérea não manter a privacidade das informações obtidas dos passageiros não constitui, em si, uma violação da secção 41712. Todavia, quando uma companhia aérea se compromete formal e publicamente a cumprir os princípios de «porto seguro» em relação à protecção da privacidade das informações que lhe são fornecidas pelos consumidores, o Department terá poderes para utilizar as competências jurídicas da secção 41712, com vista a garantir o respeito desses princípios. Por conseguinte, quando um passageiro dá informações a uma companhia que se comprometeu a honrar os princípios de «porto seguro», qualquer incumprimento poderá ser prejudicial ao consumidor e constituir uma violação da secção 41712. O serviço de que faço parte concederá a máxima prioridade à investigação e instrução de tal incumprimento. Também comunicaremos ao Department of Commerce os resultados desses processos.

Uma violação da secção 41712 pode resultar na emissão de uma decisão para fazer cessar e proibir as práticas denunciadas e na imposição de sanções de carácter civil por violação de uma decisão desse tipo. Embora não tenhamos autoridade para fixar os danos ou conceder uma compensação pecuniária aos queixosos, temos competências para aprovar soluções resultantes de investigações e processos instruídos pelo Department que tenham valor para os consumidores, quer em atenuação, quer como compensação pelas sanções pecuniárias que, de outro modo, seriam pagas. Já o fizemos, podemos fazê-lo e fá-lo-emos no contexto dos princípios de porto seguro, se as circunstâncias o justificarem. Uma violação repetida da secção 41712, por qualquer companhia aérea norte-americana, também levantará questões relativas à disposição de cumprimento da companhia que pode, em situações extremas, levar a considerar que uma companhia aérea não tem condições para operar e, consequentemente, perder a sua licença de exploração (ver DOT Orders

93-6-34 de 23 de Junho de 1993 e 93-6-11 de 9 de Junho de 1993. Embora este processo não envolvesse a secção 41712, resultou, efectivamente, na revogação da licença de exploração de uma companhia aérea, por ignorância total das disposições do Federal Aviation Act, de um acordo bilateral, e dos regulamentos e regras do Department).

Espero que estas informações tenham utilidade e estou ao inteiro dispor de Vossa Excelência para quaisquer dúvidas ou informações de que necessite.

Com os meus melhores cumprimentos,

Samuel Podberesky

Conselheiro-Geral Adjunto
Aviation Enforcement and Proceeding

ANEXO VII

Nos termos da alínea b) do n.º 2 do artigo 1.º, os entes públicos administrativos nos EUA com competência para investigar denúncias, tomar medidas contra práticas desleais e enganosas, assim como proceder à reparação de pessoas singulares, independentemente do seu país de residência ou da sua nacionalidade, sempre que exista incumprimento dos princípios aplicados em conformidade com as FAQ, são as seguintes:

1. A Federal Trade Commission

2. O Department of Transportation

A competência da Federal Trade Commission está prevista no artigo 5.º do Federal Trade Commission Act. A competência da Federal Trade Commission nos termos do artigo 5.º não abrange: bancos, instituições de poupança e crédito e cooperativas de crédito; redes de telecomunicações e sociedades de transportes interestatais, transportadoras aéreas e carregadores e entrepostos. Embora os seguros não estejam especificamente incluídos na lista de excepções do artigo 5.º, a Lei McCaran-Ferguson ([1]) deixa a regulamentação no domínio dos seguros, a cada Estado. Todavia as disposições da lei FTC aplicam-se ao domínio dos seguros na medida em que a lei de Estado não regule tal domínio. A FTC tem competência residual em matéria de actos desleais ou enganosos praticados por companhias de seguros do quadro fora da sua actividade seguradora.

A competência do Department of Transportation norte-americana está prevista no título 49 do United States Code, Section 41712. O Department of Transportation inicia processos com base nas suas investigações e em denúncias formais ou informais de indivíduos, agentes de viagens, companhias aéreas e serviços administrativos estrangeiros.

([1]) 15 U.S.C. § 1011 et seq.