COMISSÃO
EUROPEIA

Bruxelas, 27.11.2013
COM(2013) 846 final

COMUNICAÇÃO DA COMISSÃO AO PARLAMENTO EUROPEU E AO CONSELHO

Restabelecer a confiança nos fluxos de dados entre a UE e os EUA

1. INTRODUÇÃO: ALTERAÇÕES SOFRIDAS PELAS TRANSFERÊNCIAS DE DADOS ENTRE A UNIÃO EUROPEIA E OS ESTADOS UNIDOS

A União Europeia e os Estados Unidos mantêm uma parceria estratégica essencial para promovermos os nossos valores comuns, a nossa segurança e a nossa liderança partilhada no contexto mundial.

A confiança nessa parceria foi, todavia, recentemente abalada e precisa de ser restabelecida. A UE, os Estados-Membros e os cidadãos europeus manifestaram a sua profunda preocupação com as revelações sobre os programas norte-americanos de recolha de dados em grande escala, nomeadamente no que se refere à proteção dos seus dados pessoais[1]. A vigilância generalizada das comunicações privadas dos cidadãos, das empresas ou dos dirigentes políticos é inaceitável.

As transferências de dados pessoais são um elemento importante e necessário da relação transatlântica. Fazem parte integrante das trocas comerciais transatlânticas, nomeadamente nos novos setores digitais emergentes, como as redes sociais ou a computação em nuvem, implicando a transferência de uma grande quantidade de dados da UE para os EUA. São também uma componente essencial da cooperação UE-EUA em matéria de aplicação da lei e da cooperação entre os Estados-Membros e os EUA no domínio da segurança nacional. Para facilitar esse fluxo de dados, garantindo, simultaneamente, um elevado nível de proteção, como exigido pela legislação da UE, os Estados Unidos e a União Europeia já celebraram uma série de acordos e convenções.

As trocas comerciais são abordadas na Decisão 2000/520/CE[2] (a seguir designada Decisão «porto seguro»), que constitui a base jurídica das transferências de dados pessoais da UE para as empresas sedeadas nos EUA que tenham subscrito os princípios de privacidade do sistema «porto seguro».

O intercâmbio de dados pessoais UE-EUA em matéria de aplicação da lei, incluindo a prevenção e a luta contra o terrorismo e as outras formas graves de criminalidade, rege-se por uma série de acordos a nível da UE. Trata-se, nomeadamente do acordo sobre auxílio judiciário mútuo[3], do acordo sobre a utilização e a transferência dos registos de identificação dos passageiros (PNR)[4], do acordo sobre o tratamento de dados de mensagens de pagamentos financeiros e a sua transferência da União Europeia para os Estados Unidos para efeitos do Programa de Deteção do Financiamento do Terrorismo (TFTP)[5] e do acordo entre a Europol e os EUA. Os referidos acordos procuram responder a desafios importantes em matéria de

---

1 Para efeitos da presente comunicação, as referências aos cidadãos da UE incluem igualmente os nacionais de países terceiros abrangidos pelo âmbito de aplicação da legislação de proteção de dados da União Europeia.

2 Decisão da Comissão 2000/520/CE, de 26 de julho de 2000, nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho e relativa ao nível de proteção assegurado pelos princípios de «porto seguro» e pelas respetivas questões mais frequentes (FAQ) emitidos pelo *Department of Commerce* dos Estados Unidos da América

3 Decisão 2009/820/PESC do Conselho, de 23 de outubro de 2009, relativa à celebração, em nome da União Europeia, do Acordo entre a União Europeia e os Estados Unidos da América sobre extradição e do Acordo entre a União Europeia e os Estados Unidos da América sobre auxílio judiciário mútuo, JO L 291 de 7.11. 2009, p. 40.

4 Decisão do Conselho 2012/472/UE, de 26 de abril de 2012, relativa à celebração do Acordo entre os Estados Unidos da América e a União Europeia sobre a utilização e a transferência dos registos de identificação dos passageiros para o Departamento da Segurança Interna dos Estados Unidos, JO L 215 de 11.8.2012, p. 4.

5 Decisão do Conselho de 13 de julho de 2010 relativa à celebração do Acordo entre a União Europeia e os Estados Unidos da América sobre o tratamento de dados de mensagens de pagamentos financeiros e a sua transferência da União Europeia para os Estados Unidos para efeitos do Programa de Deteção do Financiamento do Terrorismo, JO L 195 de 27.7.2010, p. 3.

segurança e satisfazer os interesses comuns em matéria de segurança da UE e dos EUA, assegurando simultaneamente um elevado nível de proteção dos dados pessoais. Além disso, a UE e os EUA estão atualmente a negociar um acordo-quadro sobre proteção de dados no domínio da cooperação policial e judiciária (a seguir designado «acordo-quadro global»)[6], com o objetivo de assegurar um nível elevado de proteção dos cidadãos cujos dados sejam transferidos e, assim, reforçar a cooperação UE-EUA na luta contra a criminalidade e o terrorismo, com base em valores comuns e nas garantias definidas de comum acordo.

Estes instrumentos são aplicados num contexto em que os fluxos de dados pessoais assumem uma importância cada vez maior.

Por um lado, o desenvolvimento da economia digital gerou um crescimento exponencial da quantidade, da qualidade, da diversidade e da natureza das atividades de tratamento de dados. Os cidadãos utilizam cada vez mais os serviços de comunicação eletrónicos na sua vida quotidiana. Os dados pessoais tornaram-se um bem extremamente valioso: o valor estimado dos dados dos cidadãos da UE foi de 315 mil milhões de EUR em 2011, com potencial de crescer até quase um bilião de EUR anuais até 2020[7]. O mercado da análise dos grandes conjuntos de dados regista um crescimento global anual de 40%[8]. Do mesmo modo, a evolução tecnológica, nomeadamente a relacionada com a computação em nuvem, realça a importância da noção de transferência de dados internacional à medida que os fluxos de dados transnacionais se tornam uma realidade quotidiana[9].

O aumento da utilização das comunicações eletrónicas e dos serviços de tratamento de dados, nomeadamente a computação em nuvem, veio alargar consideravelmente o âmbito e a importância das transferências de dados transatlânticas. Alguns aspetos, nomeadamente a posição central das empresas norte-americanas na economia digital[10], o tráfego transatlântico de grande parte das comunicações eletrónicas e o volume dos fluxos eletrónicos de dados entre a UE e os EUA, tornaram-se ainda mais importantes.

Por outro lado, os novos métodos de tratamento dos dados pessoais suscitam questões novas e pertinentes. Isto aplica-se tanto aos novos meios de tratamento em grande escala dos dados dos consumidores pelas empresas privadas para fins comerciais, como ao aumento da capacidade dos serviços de informações para efetuarem uma vigilância em grande escala das comunicações.

Os programas norte-americanos de recolha de informações em grande escala, como o PRISM, afetam os direitos fundamentais dos cidadãos europeus e, nomeadamente o direito à privacidade e à proteção dos dados pessoais. Estes programas também indiciam a existência de uma ligação entre a vigilância governamental e o tratamento de dados pelas empresas privadas, nomeadamente pelas empresas de Internet norte-americanas, o que pode, assim, ter impacto económico. O facto de os utilizadores da Internet recearem o tratamento em grande escala dos seus dados pessoais pelas empresas privadas ou a vigilância dos seus dados pelos

---

6 O Conselho adotou em 3 de dezembro de 2010 a decisão que autoriza a Comissão a negociar o acordo. Ver IP/10/1661 de 3 de dezembro de 2010.

7 Ver Boston Consulting Group, «*The Value of our Digital Identity*», novembro de 2012.

8 Ver McKinsey, «*Big data: The next frontier for innovation, competition, and productivity*», 2011.

9 Comunicação «Explorar plenamente o potencial da computação em nuvem na Europa», COM(2012) 529 final

10 Por exemplo, em junho de 2012 o número global de visitantes únicos das páginas do Microsoft Hotmail, Google Gmail e Yahoo! Mail a partir dos países europeus elevou-se a mais de 227 milhões, eclipsando todos os outros fornecedores de serviços. O número acumulado de utilizadores únicos europeus que acederam ao Facebook e ao Facebook Mobile em março de 2012 foi de 196,5 milhões, fazendo do Facebook a maior rede social na Europa. O Google é o motor de busca mais utilizado, sendo o preferido de 90,2% dos utilizadores da Internet em todo o mundo. Em junho de 2013, o serviço norte-americano de mensagens móveis What's App foi utilizado por 91% dos utilizadores de iPhone na Alemanha.

serviços de informações pode prejudicar a sua confiança na economia digital e ter efeitos negativos no crescimento.
Estes desenvolvimentos vieram colocar novos desafios ao intercâmbio de dados UE-EUA. A presente comunicação pretende dar uma resposta a esses desafios, explorando vias que possam ser seguidas com base nas conclusões do relatório dos copresidentes da UE do grupo de trabalho *ad hoc* UE-EUA sobre proteção de dados, assim como na comunicação relativa ao sistema «porto seguro».
A presente comunicação visa encontrar formas eficazes de restabelecer a confiança e aprofundar a cooperação UE-EUA neste domínio, reforçando a globalidade das relações transatlânticas.

A presente comunicação parte do princípio de que o nível de proteção dos dados pessoais deve ser abordado no seu contexto próprio, sem prejudicar as outras dimensões das relações UE-EUA, incluindo as negociações atualmente em curso da Parceria Transatlântica de Comércio e Investimento. Por esse motivo, as normas em matéria de proteção dos dados não serão negociadas no âmbito da Parceria Transatlântica, que deve respeitar integralmente as normas de proteção de dados.

Importa referir que enquanto a UE só pode tomar medidas nos domínios em que possua competência, nomeadamente para salvaguardar a aplicação do direito da UE[11], a segurança nacional continua a ser uma competência exclusiva de cada Estado-Membro[12].

2. IMPACTO NOS INSTRUMENTOS DE TRANSFERÊNCIA DE DADOS

Em primeiro lugar, no que se refere aos dados transferidos para fins comerciais, o sistema «porto seguro» mostrou ser um importante instrumento de transferência de dados entre a União Europeia e os Estados Unidos. A sua importância comercial tem vindo a aumentar à medida que os fluxos de dados pessoais assumem maior importância na relação comercial transatlântica. Nos último 13 anos, o sistema passou a abranger mais de 3 000 empresas, mais de metade das quais aderiram nos últimos 5 anos. No entanto, aumentou a preocupação com o nível de proteção dos dados pessoais dos cidadãos da UE que são transferidos para os EUA através deste sistema. A adesão voluntária e o seu caráter declaratório fizeram com que a atenção se centrasse na transparência e na aplicação efetiva do sistema. Embora a maioria das empresas norte-americanas aplique os princípios do sistema «porto seguro», algumas empresas autocertificadas não o fazem. A violação dos princípios de privacidade do sistema por algumas empresas autocertificadas confere-lhes vantagens competitivas face às empresas europeias que operam nos mesmos mercados.
Além disso, pese embora o sistema «porto seguro» preveja a possibilidade de impor derrogações às normas de proteção dos dados por motivos de segurança nacional[13], coloca-se a questão de saber se a recolha e o tratamento de dados pessoais ao abrigo dos programas de vigilância dos EUA são necessários e proporcionados para satisfazer os interesses nacionais em matéria de segurança. Ficou também claro, com as conclusões do grupo de trabalho *ad hoc* UE-EUA que, no âmbito desses programas, os cidadãos da UE não beneficiam dos mesmos direitos e garantias processuais que os cidadãos norte-americanos.
O alcance desses programas de vigilância, juntamente com a desigualdade de tratamento dos cidadãos da UE, compromete o grau de proteção conferido pelo acordo «porto seguro». Os dados pessoais dos cidadãos da UE enviados para os EUA através do sistema podem ser

[11] Ver o acórdão proferido pelo Tribunal de Justiça da União Europeia no processo C-300/11, ZZ contra *Secretary of State for the Home Department*.
[12] Artigo 4.°, n.º 2, do Tratado da União Europeia.
[13] Ver, por exemplo, a Decisão «porto seguro», anexo I.

acedidos e posteriormente tratados pelas autoridades dos EUA de uma forma que é incompatível com os motivos pelos quais esses dados foram originalmente recolhidos na UE e com os fins para os quais foram transferidos para os EUA. A maioria das empresas de Internet norte-americanas mais diretamente envolvidas nestes programas são certificadas ao abrigo do sistema «porto seguro».

Em segundo lugar, no que se refere ao intercâmbio de dados para fins coercivos, os acordos existentes (PNR, TFTP) mostraram ser adequados para abordar as ameaças comuns à segurança relacionadas com o terrorismo e a criminalidade grave transnacional, prevendo garantias que asseguram um elevado nível de proteção dos dados[14]. Essas garantias são extensivas aos cidadãos da UE, estando previstos mecanismos para avaliar a sua aplicação e resolver as eventuais questões que suscitem preocupação. O Acordo TFTP contempla ainda um sistema de controlo, segundo o qual supervisores independentes da UE podem verificar a forma como os Estados Unidos pesquisam os dados abrangidos pelo acordo.

Dada a grande preocupação suscitada na UE pelos programas de vigilância dos EUA, a Comissão Europeia decidiu utilizar os referidos mecanismos para verificar a forma como esses acordos são aplicados. No caso do Acordo PNR, foi efetuado um reexame conjunto, em que participaram especialistas em proteção de dados da UE e dos EUA, a fim de avaliar a forma como o acordo era aplicado[15]. Esse reexame não encontrou qualquer indicação de que os programas de vigilância dos EUA cobrissem os dados dos passageiros abrangidos pelo acordo PNR ou tivessem qualquer impacto sobre estes. No caso do Acordo TFTP, a Comissão deu início a consultas formais após ter sido alegado que os serviços de informações teriam acesso direto a dados pessoais na UE, violando assim o disposto no acordo. Essas consultas não permitiram encontrar qualquer elemento que comprove a violação do Acordo TFTP, tendo os EUA prestado garantias por escrito de que não fora efetuada qualquer recolha direta de dados em violação do acordo.

O grande volume de dados pessoais recolhidos e tratados pelos programas de vigilância norte-americanos exige, contudo, que se continue a assegurar futuramente um controlo rigoroso da aplicação dos acordos PNR e TFTP. A UE e os EUA acordaram, por conseguinte, em antecipar para a primavera de 2014 o próximo reexame conjunto do Acordo TFTP. No âmbito desse reexame, assim como no dos seguintes, deve ser aumentada a transparência do funcionamento do sistema de supervisão e da proteção dos dados dos cidadãos da UE. Paralelamente, serão tomadas medidas para assegurar que o sistema de supervisão continua a prestar especial atenção à forma como são tratados os dados transferidos para os EUA ao abrigo do acordo, com especial incidência na forma como são partilhados entre as autoridades norte-americanas.

Em terceiro lugar, o aumento do volume de dados pessoais que são objeto de tratamento aumenta a importância das garantias jurídicas e administrativas aplicáveis. Um dos objetivos do grupo de trabalho *ad hoc* UE-EUA consistia em determinar que garantias poderiam ser aplicadas para minimizar o impacto do tratamento dos dados em termos dos direitos fundamentais dos cidadãos da UE. Convém igualmente dispor de garantias para proteger as empresas. Alguns atos legislativos dos EUA, nomeadamente o *Patriot Act*, permitem que as autoridades norte-americanas solicitem diretamente às empresas acesso a dados armazenados na UE. Consequentemente, as empresas europeias, assim como as empresas norte-americanas

[14] Ver relatório conjunto da Comissão e do Departamento do Tesouro dos EUA sobre o valor dos dados fornecidos no quadro do TFTP, nos termos do artigo 6.º, n.º 6, do Acordo entre a União Europeia e os Estados Unidos da América sobre o tratamento de dados relativos a mensagens de pagamentos e sua transferência da União Europeia para os Estados Unidos para efeitos do Programa de Deteção do Financiamento do Terrorismo.

[15] Ver relatório da Comissão «Reexame conjunto da aplicação do Acordo entre a União Europeia e os Estados Unidos da América sobre a utilização e a transferência dos dados do registo de identificação dos passageiros para o Departamento da Segurança Interna dos Estados Unidos».

presentes na UE, podem ser obrigadas a transferir dados para os EUA em violação da legislação da UE e dos Estados-Membros, confrontando-se com um conflito de obrigações jurídicas. A insegurança jurídica gerada por essa situação pode entravar o desenvolvimento de novos serviços digitais, como a computação em nuvem, que oferecem soluções mais eficazes e económicas para os cidadãos e as empresas.

3. ASSEGURAR UMA PROTEÇÃO EFICAZ DOS DADOS PESSOAIS

A transferência de dados pessoais entre a UE e os EUA é uma componente essencial das relações comerciais transatlânticas. A partilha de informações é outra componente essencial da cooperação UE-EUA em matéria de segurança, a qual é decisiva para se atingir o objetivo comum da prevenção e luta contra a criminalidade grave e o terrorismo. As recentes revelações sobre os programas de recolha de informações dos EUA vieram abalar, contudo, a confiança em que esta cooperação deve assentar e, nomeadamente, a confiança no tratamento dos dados pessoais. Para se poder restabelecer a confiança nas transferências de dados, em benefício da economia digital, da segurança, tanto da UE como dos EUA, e, das relações transatlânticas em geral, importa adotar as medidas a seguir enumeradas.

3.1. Reforma das normas da UE em matéria de proteção de dados

A reforma das normas europeias da proteção de dados apresentada pela Comissão Europeia em janeiro de 2012[16] constitui uma resposta clara no que se refere à proteção dos dados pessoais. Cinco componentes dessa proposta assumem especial importância.

Em primeiro lugar, no que respeita ao seu âmbito de aplicação territorial, o regulamento proposto clarifica que as empresas que não estão estabelecidas na União têm de aplicar a legislação de proteção de dados da UE sempre que ofereçam bens ou serviços a consumidores europeus ou pretendam observar o seu comportamento. Por outras palavras, o direito fundamental à proteção dos dados pessoais será respeitado independentemente da localização geográfica da empresa ou do serviço de tratamento de dados[17].

Em segundo lugar, no que se refere às transferências internacionais, o regulamento proposto estabelece as condições em que os dados podem ser transferidos para fora da UE. Essas transferências só podem ser autorizadas se forem satisfeitas essas condições, as quais asseguram às pessoas um elevado nível de proteção[18].

Em terceiro lugar, no que respeita ao cumprimento das normas, as disposições propostas preveem sanções proporcionadas e dissuasivas (até 2 % do volume de negócios global anual

---

16 COM(2012) 10 final: Proposta de diretiva do Parlamento Europeu e do Conselho relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou de execução de sanções penais, e à livre circulação desses dados, Bruxelas, 25.1.2012, e COM(2012) 11 final: Proposta de Regulamento do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (regulamento geral sobre a proteção de dados).

17 A Comissão tomou nota de que o Parlamento Europeu confirmou e reforçou este importante princípio, consagrado no artigo 3.º do regulamento proposto, na sua votação de 21 de outubro de 2013 relativa ao relatório sobre a reforma da proteção de dados elaborado pelos membros de Parlamento Jan-Philipp Albrecht e Dimitrios Droutsas na Comissão das Liberdades Cívicas, da Justiça e dos Assuntos Internos (LIBE).

18 A Comissão tomou nota de que, na sua votação de 21 de outubro de 2013, a Comissão LIBE do Parlamento Europeu propôs que fosse incluída uma disposição no futuro regulamento que sujeitaria os pedidos apresentados por autoridades estrangeiras para aceder a dados pessoais recolhidos na UE à obtenção de uma autorização prévia da autoridade nacional de proteção de dados, sempre que o pedido seja formulado fora do âmbito de um tratado de auxílio judiciário mútuo ou qualquer outro acordo internacional.

da empresa em causa) a fim de garantir que as empresas cumprem a legislação da UE[19]. A existência de sanções credíveis aumenta o incentivo para que as empresas cumpram a legislação da UE.

Em quarto lugar, o regulamento proposto prevê normas claras sobre as obrigações e responsabilidades, nomeadamente em termos de segurança, dos subcontratantes, nomeadamente os fornecedores de serviços de computação em nuvem[20]. Como evidenciado pelos dados revelados sobre os programas de recolha de informações dos EUA, este aspeto é essencial, dado que esses programas afetam os dados armazenados na nuvem. Por outro lado, as empresas que fornecem espaço de armazenamento na nuvem e às quais as autoridades estrangeiras solicitam dados pessoais não podem eximir-se às suas responsabilidades invocando a sua qualidade de meros subcontratantes e não de «responsáveis pelo tratamento dos dados».

Por último, as novas medidas legislativas permitirão estabelecer normas abrangentes para proteger os dados pessoais objeto de tratamento para efeitos de aplicação coerciva da lei.

Prevê-se que as referidas medidas legislativas sejam adotadas no decurso de 2014[21].

3.2. Garantir uma maior segurança do sistema «porto seguro»

O sistema «porto seguro» é um elemento importante das relações comerciais UE-EUA e é utilizado por empresas de ambos os lados do Atlântico.

O relatório da Comissão sobre o funcionamento do sistema permitiu identificar algumas deficiências. Em virtude de falta de transparência e de controlo da sua aplicação, alguns membros autocertificados não respeitam, na prática, os princípios do sistema. Esta situação tem efeitos negativos para os direitos fundamentais dos cidadãos da UE. Cria igualmente uma desvantagem para as empresas europeias em relação às suas congéneres dos EUA que exercem a sua atividade ao abrigo do sistema mas que, na prática, não aplicam os referidos princípios. Esta deficiência do sistema prejudica ainda a maior parte das empresas norte-americanas que aplicam corretamente os princípios do sistema. O sistema «porto seguro» funciona igualmente como um canal para transferir dados pessoais dos cidadãos da UE para os EUA pelas empresas que estão obrigadas a fornecer dados aos serviços de informações norte-americanos no âmbito dos programas de recolha de informações dos EUA. Se não forem corrigidas, as referidas deficiências criam uma desvantagem competitiva para as empresas da UE e podem comprometer o direito fundamental dos cidadãos da UE à proteção dos seus dados pessoais.

As deficiências do sistema foram sublinhadas pela resposta dada pelas Autoridades Europeias de Proteção de Dados às recentes revelações sobre a vigilância de dados pessoais. O artigo 3.º da Decisão «porto seguro» autoriza essas autoridades a suspender, em determinadas condições, os fluxos de dados para as empresas certificadas[22]. Os comissários responsáveis

---

19 A Comissão tomou nota de que, na sua votação de 21 de outubro de 2013, a Comissão LIBE propôs o reforço da proposta da Comissão prevendo que as multas possam ascender a 5% do volume de negócios global anual da empresa.

20 A Comissão tomou nota de que, na sua votação de 21 de outubro de 2013, a Comissão LIBE subscreveu o reforço das obrigações e responsabilidades dos subcontratantes, nomeadamente no que se refere ao artigo 26.º do regulamento proposto.

21 Nas Conclusões do Conselho Europeu de outubro de 2013 afirma-se: «É importante fomentar a confiança dos cidadãos e das empresas na economia digital. A adoção atempada de um sólido quadro geral da UE em matéria de proteção de dados e da diretiva relativa à cibersegurança é essencial para a realização do mercado único digital até 2015».

22 Mais concretamente, nos termos do artigo 3.º da Decisão «porto seguro», essa suspensão pode ter lugar nos casos em que existam fortes probabilidades para supor que os princípios não estão a ser respeitados; haja 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; a continuação da transferência dos dados possa causar graves prejuízos às pessoas em causa; e as entidades competentes nos Estados-Membros tiverem

pela proteção dos dados na Alemanha decidiram não emitir novas autorizações de transferência de dados para países que não pertençam à UE (por exemplo, para a utilização de certos serviços em nuvem). Irão ainda analisar se se deve suspender a transferência de dados com base nos princípios «porto seguro»[23]. O risco daqui decorrente é que essas medidas, adotadas a nível nacional, possam criar diferenças a nível do âmbito de aplicação do sistema, o que significaria que o «porto seguro» deixaria de ser um mecanismo essencial para a transferência de dados pessoais entre a UE e os EUA.

Nos termos da Diretiva 95/46/CE, a Comissão pode suspender ou revogar a Decisão «porto seguro» se o sistema deixar de proporcionar um adequado nível de proteção. Além disso, nos termos do artigo 3.º da Decisão «porto seguro», a Comissão pode revogar, suspender ou limitar o âmbito de aplicação da Decisão, e, nos termos do artigo 4.º, pode adaptar a Decisão em qualquer altura em função da experiência proporcionada pela sua aplicação.

Neste contexto, podem ser analisadas diversas alternativas, nomeadamente:

- a manutenção do *status quo*;
- o reforço do sistema «porto seguro» e a revisão aprofundada do seu funcionamento;
- a suspensão ou a revogação da Decisão «porto seguro».

Dadas as deficiências identificadas, não se pode continuar a aplicar o sistema como tem vindo a ser aplicado até à data. No entanto, a sua revogação afetaria negativamente os interesses das empresas, tanto da UE como dos EUA, que são membros do sistema. A Comissão considera que o sistema «porto seguro» deveria antes ser reforçado.

As alterações a introduzir devem abordar as deficiências estruturais relacionadas com a transparência e o cumprimento das regras do sistema, os princípios materiais «porto seguro» e o recurso à derrogação por motivos de segurança nacional.

Concretamente, para que o sistema possa funcionar como previsto, o controlo e a supervisão pelas autoridades dos EUA da conformidade das empresas certificadas com os princípios de privacidade «porto seguro» deve ser mais eficaz e sistemático. A transparência das políticas de proteção da vida privada das empresas certificadas deve ser melhorada. Deve igualmente proporcionar-se a todos os cidadãos da UE o acesso a mecanismos de resolução de litígios.

A Comissão vai encetar urgentemente um diálogo com as autoridades dos EUA para debater as deficiências identificadas. Até ao verão de 2014 deverá ser encontrada uma solução, que deve ser aplicada o mais rapidamente possível. Com base nessa solução, a Comissão procederá a uma análise aprofundada do funcionamento do «porto seguro». O reexame do funcionamento do sistema incluirá uma consulta pública e a realização de debates no Parlamento Europeu e no Conselho, assim como negociações com as autoridades norte-americanas.

É igualmente importante que a derrogação por motivos de segurança nacional prevista na Decisão «porto seguro» só seja utilizada na medida do necessário e de forma proporcionada.

3.3. Reforçar as garantias em matéria de proteção dos dados no âmbito da cooperação em matéria de aplicação da lei

A UE e os EUA estão atualmente a negociar um acordo-quadro global de proteção de dados relativo à transferência e ao tratamento de dados pessoais no âmbito da cooperação policial e judiciária em matéria penal. A conclusão desse acordo, que prevê um elevado nível de proteção dos dados pessoais, contribuiria grandemente para o reforço da confiança entre as

---

envidado esforços razoáveis, dadas as circunstâncias, para facultar à organização em causa a informação e oportunidade necessárias para responder.

[23] *Bundesbeauftragten für den Datenschutz und die Informationsfreiheit*, comunicado de imprensa de 24 de julho de 2013.

duas margens do Atlântico. Ao aumentar a proteção dos direitos dos cidadãos da UE em matéria de dados pessoais, contribuiria igualmente para um reforço da cooperação transatlântica destinada a prevenir e a combater a criminalidade e o terrorismo.

Segundo a decisão que autoriza a Comissão a negociar o referido acordo, as negociações devem ter por objetivo um elevado nível de proteção, em consonância com o acervo da UE em matéria de proteção de dados, traduzindo-se na adoção de normas e garantias, nomeadamente quanto à limitação da finalidade do tratamento dos dados, às condições e à duração do período de conservação dos dados. Nessas negociações, a Comissão deve ainda obter compromissos quanto aos direitos suscetíveis de aplicação coerciva, incluindo os mecanismos de recurso judicial para os cidadãos da UE que não residam nos EUA[24]. A estreita cooperação UE-EUA relativamente às ameaças à sua segurança comum deve abranger os esforços para garantir que os cidadãos de ambos os lados do Atlântico beneficiam dos mesmos direitos quando sejam tratados dados idênticos para os mesmos fins. É igualmente importante definir rigorosamente as derrogações impostas por motivos de segurança, assim como definir as garantias e as limitações.

As referidas negociações constituem a oportunidade de clarificar que os dados pessoais detidos por empresas privadas situadas na UE não podem ser diretamente acedidos ou transferidos para autoridades com funções coercivas norte-americanas sem ser através das vias formais de cooperação, nomeadamente os acordos de auxílio judiciário mútuo ou os acordos setoriais UE-EUA que autorizam este tipo de transferência. O acesso por outros meios deve ser excluído, salvo se tiver lugar em situações claramente definidas, de caráter excecional e suscetíveis de recurso judicial. Os EUA devem assumir compromissos nesse sentido[25].

Um acordo-quadro que respeite estas indicações pode proporcionar o enquadramento geral para garantir um elevado nível de proteção dos dados pessoais transferidos para os EUA a fim de prevenir ou combater a criminalidade e o terrorismo. Sempre que necessário, em função do tipo de dados em causa, a celebração de acordos setoriais pode estabelecer normas e garantias suplementares, inspirando-se no exemplo dos acordos TFTP e PNR entre a UE e os EUA, que estabelecem condições rigorosas para a transferência de dados, prevendo garantias para os cidadãos da UE.

3.4. Acautelar as preocupações europeias no processo de reforma atualmente em curso nos EUA

---

[24] Ver a passagem em questão da declaração conjunta à imprensa na sequência da reunião ministerial «Justiça e Assuntos Internos» UE-EUA de 18 de novembro de 2013 em Washington: «Estamos, por conseguinte, empenhados, em efetuar progressos urgentes na negociação de um acordo-quadro global significativo e abrangente para a proteção de dados no domínio da aplicação coerciva da lei. Esse acordo deve proporcionar uma base para facilitar as transferências de dados no contexto da cooperação policial e judiciária em matéria penal, assegurando um elevado nível de proteção dos dados pessoais dos cidadãos dos EUA e da UE. Estamos também empenhados em resolver as questões suscitadas por ambas as partes, incluindo a questão das vias de recurso jurisdicional (uma questão que é crítica para a UE). O objetivo é concluir as negociações desse acordo antes do verão de 2014».

[25] Ver a passagem em questão da declaração conjunta à imprensa na sequência da reunião ministerial «Justiça e Assuntos Internos» UE-EUA de 18 de novembro de 2013 em Washington: «Sublinhamos igualmente a importância do acordo de auxílio judiciário mútuo UE-EUA. Reiteramos o nosso empenho em assegurar a sua utilização ampla e efetiva para efeitos de prova em processo penal. Debatemos igualmente a necessidade de clarificar que os dados pessoais detidos por entidades privadas no território da outra parte não podem ser acedidos pelas autoridades com funções coercivas sem ser pelos canais devidamente autorizados. Concordámos ainda em rever o funcionamento do acordo de auxílio judiciário mútuo, tal como previsto no acordo, e em proceder a consultas reciprocas sempre que tal se mostre necessário».

O Presidente Obama anunciou um reexame das atividades das autoridades de segurança nacional dos EUA, incluindo do enquadramento jurídico em vigor. Esse processo, atualmente em curso, constitui uma excelente oportunidade para abordar as preocupações suscitadas na UE pelas recentes revelações sobre os programas de recolha de informações norte-americanos. As principais alterações consistiriam em alargar as garantias concedidas aos cidadãos norte-americanos e residentes nos EUA aos cidadãos da União Europeia que não residem nos EUA, garantir maior transparência das atividades dos serviços de informações e reforçar o seu controlo. Essas alterações devem contribuir para restaurar a confiança no intercâmbio de dados UE-EUA e para promover a utilização da Internet pelos cidadãos europeus.

No que se refere à extensão aos cidadãos da UE das garantias reconhecidas aos cidadãos e residentes nos EUA, importa reexaminar as normas jurídicas relativas aos programas de vigilância dos EUA que tratam diferentemente os cidadãos dos EUA e os da UE, nomeadamente em função dos princípios da necessidade e da proporcionalidade e tendo em conta a estreita parceria de segurança transatlântica, que assenta em valores, direitos e liberdades comuns. Isto poderia contribuir para que os cidadãos europeus fossem menos afetados pelos programas de recolha de informações norte-americanos.

É necessária maior transparência quanto ao enquadramento jurídico dos programas de recolha de informações dos EUA e à interpretação do mesmo pelos tribunais norte-americanos, assim como quanto à dimensão quantitativa dos referidos programas. Os cidadãos da UE beneficiariam igualmente dessas alterações.

O controlo dos programas de recolha de informações poderia ser melhorado mediante o reforço do papel do *Foreign Intelligence Surveillance Court* norte-americano e a introdução da possibilidade de os particulares interporem recursos. Esses mecanismos poderiam reduzir o tratamento de dados pessoais dos cidadãos europeus que não sejam pertinentes para efeitos de segurança nacional.

3.5. Promover a adoção de normas internacionais de proteção da privacidade

Os problemas relacionados com os métodos modernos de proteção de dados não se limitam às transferências de dados entre a UE e os EUA. Qualquer pessoa tem direito a um elevado nível de proteção dos seus dados pessoais. As normas da UE em matéria de recolha, tratamento e transferência de dados pessoais devem ser promovidas internacionalmente.

Recentemente, foram propostas várias iniciativas para aumentar a proteção da privacidade, nomeadamente na Internet[26]. A UE deve garantir que, caso essas iniciativas avancem, terão plenamente em conta os princípios da proteção dos direitos fundamentais, da liberdade de expressão e da privacidade dos dados pessoais consagrados na legislação da UE, assim como a estratégia da UE em matéria de cibersegurança, sem comprometer a liberdade, a abertura e a segurança do ciberespaço. Isto implica um modelo de governação em que os vários intervenientes possam participar de uma forma democrática e eficaz.

As reformas em curso da legislação de proteção dos dados pessoais de ambos os lados do Atlântico proporcionam à UE e aos EUA uma oportunidade única para estabelecerem uma norma internacional. Os intercâmbios transatlânticos de dados, assim como os intercâmbios com outros países, beneficiariam grandemente do reforço do enquadramento jurídico interno dos EUA, nomeadamente da adoção da «*Consumer Privacy Bill of Rights*» (a declaração de direitos sobre a proteção da privacidade dos consumidores), apresentada pelo Presidente Obama em fevereiro de 2012 no âmbito de um programa global destinado a melhorar a proteção da privacidade dos consumidores. A existência de um conjunto sólido de normas de proteção dos dados pessoais possuindo força executória e reconhecidas tanto na UE como nos EUA constituiria uma base sólida para os fluxos transnacionais de dados.

[26] Ver o projeto de resolução apresentado à Assembleia Geral das Nações Unidas pela Alemanha e pelo Brasil, apelando à proteção da privacidade tanto *online* como *offline*.

A fim de promover as normas internacionais de proteção da privacidade, convém igualmente promover a adesão à Convenção do Conselho da Europa relativa à proteção das pessoas no que diz respeito ao processamento de dados pessoais («Convenção 108»), que está aberta à adesão dos países que não são membros do Conselho da Europa[27]. As salvaguardas e garantias acordadas no âmbito das instâncias internacionais devem proporcionar um elevado nível de proteção, compatível com o exigido pela legislação da UE.

4. CONCLUSÕES E RECOMENDAÇÕES

As questões suscitadas na presente comunicação requerem a adoção de medidas por parte dos Estados Unidos, por parte da União Europeia, bem como pelos Estados-Membros.

As preocupações suscitadas pelo intercâmbio transatlântico de dados provocaram, acima de tudo, uma tomada de consciência quanto à necessidade de a UE e os Estados-Membros procederem rápida e ambiciosamente a uma reforma das normas de proteção dos dados pessoais. Revelaram ainda a necessidade de se dispor de um sólido enquadramento legislativo, com normas claras e com força executória mesmo que os dados sejam transferidos para o estrangeiro. As instituições da UE devem, por conseguinte, prosseguir os esforços para reformar a legislação de proteção de dados da UE até à primavera de 2014, a fim de garantir que os dados pessoais são protegidos de forma eficaz e abrangente.

Dada a importância dos fluxos de dados transatlânticos, é essencial que os instrumentos que servem de base a este intercâmbio abordem adequadamente os desafios e as oportunidades da era digital e os novos desenvolvimentos tecnológicos, nomeadamente a computação em nuvem. Os acordos e convenções, atuais ou futuros, devem garantir a continuidade de um elevado nível de proteção nos intercâmbios entre as duas margens do Atlântico.

Os cidadãos e as empresas da UE e dos EUA têm todo o interesse em que o sistema «porto seguro» funcione eficazmente e seja reforçado, mediante um melhor controlo e execução a curto prazo e um reexame aprofundado do seu funcionamento. Serão necessárias melhorias para garantir o cumprimento dos objetivos iniciais da Decisão «porto seguro», designadamente a continuidade da proteção dos dados, a segurança jurídica e a livre circulação de dados entre a UE e os EUA.

Essas melhorias devem centrar-se na necessidade de as autoridades norte-americanas controlarem e supervisionarem com mais eficácia o cumprimento pelas empresas autocertificadas dos princípios de privacidade do sistema.

É igualmente importante que a derrogação por motivos de segurança nacional, prevista na Decisão «porto seguro», só seja aplicada na medida em que seja estritamente necessária e proporcionada.

No que se refere ao cumprimento da lei, as negociações atuais de um acordo-quadro global deverão proporcionar um elevado nível de proteção aos cidadãos de ambos lados do Atlântico. A conclusão desse acordo reforçaria a confiança dos europeus no intercâmbio de dados UE-EUA e permitiria desenvolver a cooperação e a parceria em matéria de segurança. No âmbito dessas negociações devem ser assumidos compromissos no sentido de se conceder garantias processuais, incluindo vias de recurso jurisdicional, aos cidadãos europeus não residentes nos EUA.

Importa ainda obter o compromisso da administração norte-americana pelo qual os dados pessoais detidos por entidades privadas da UE não serão diretamente acessíveis aos organismos com poderes coercivos dos EUA sem ser através das vias formais de cooperação (nomeadamente os acordos de auxílio judiciário mútuo e os acordos setoriais UE-EUA, designadamente o PNR e o TFTP, que autorizam essa transferência mediante condições rigorosas), salvo em casos excecionais claramente definidos e suscetíveis de recurso judicial.

[27] Os EUA já são parte noutra convenção do Conselho da Europa: a Convenção sobre o Cibercrime, de 2001 (também designada por «Convenção de Budapeste»).

Os Estados Unidos devem ainda alargar aos cidadãos da UE que não residem nos EUA as garantias que são reconhecidas aos cidadãos norte-americanos e aos residentes nos EUA, bem como garantir que os programas de recolha de dados respeitam os princípios da necessidade e da proporcionalidade e uma maior transparência e controlo do enquadramento jurídico aplicável às autoridades de segurança norte-americanas.

Os domínios de intervenção enumerados na presente comunicação requerem um envolvimento construtivo de ambos os lados do Atlântico. Em conjunto, enquanto parceiros estratégicos, a União Europeia e os Estados Unidos devem poder ultrapassar as tensões atualmente existentes na relação transatlântica e restabelecer a confiança nos seus fluxos de dados UE-EUA. A assunção de compromissos políticos e jurídicos comuns quanto ao aprofundamento da cooperação nestes domínios contribuirá para reforçar as relações transatlânticas.